Sensorsoft®

Sensorsoft® Alert™

The Standalone Network Appliance for Environmental Monitoring

User Manual

For models SSA7001, SSA7004 and SSA7008
With Image Build Number 13 or Higher

Manual P/N 071-0084 Rev 21 January 2, 2015

Copyright © 2004-2015 Sensorsoft Corporation, All rights reserved.
Sensorsoft, Remote Watchman and Alert are trademarks of Sensorsoft Corporation.

Warning: This manual should only be used for Sensorsoft Alert running image build 13 or higher. To upgrade your appliance's image to the latest version, please follow the link below:

http://www.sensorsoft.com/ssalert_images.html

Table of Contents

About This Manual 7
Glossary of Acronyms 8
Overview 9
Software specifications and features 10
SSA7001 10
SSA7004 and SSA7008 11
Hardware specifications 12
SSA7001 12
SSA7004 and SSA7008 12
Safety Instructions 13
Working inside the Sensorsoft Alert Appliance 13
Replacing the Battery 13
FCC & DOC Notice 14
FCC Warning Statement 14
Canadian DOC Notice 14
Alert Quick Start 15
Accessing the Alert appliance using DHCP 15
Connecting to the Alert serial port console 16
Model SSA7001 16
Models SSA7004 and SSA7008 17
Configuring IP settings of the Alert Appliance 17
Connecting Sensorsoft devices to the Alert Appliance 18
Model SSA7001 18
Models SSA7004 and SSA7008 19
Alert web interface 20
Accounts and passwords 20
Logging into the Alert web interface 20
Changing web login passwords: 21
Recovering from a lost web administrator password 21
Setting date and time 22
Shutting down or rebooting the Alert Appliance 23
Monitoring a Sensorsoft Device 23
Monitoring a non-Sensorsoft Device with Plug-in Support 24
The View Monitor List Page 25
Monitor List Auto-Refresh Interval 26
Displaying Device Variables on the View Monitor List 26
Logging Variable Readings to Data Log File 27
Logging Data 29
Status and Error Logs 29
Data file Naming Convention 29
Graphing data files 30
Viewing log files 30
Logging Data on a NFS Server 30
Setting up Alerts 32

Setting up Alerting Limits for Device Variables....32
Setting up Email Alerts....33
SMTP Settings....33
Setting up Email Alerts for Device Variables....34
Setting up Pager Alerts....36
Connecting a Modem to the Alert Appliance....36
Paging Settings....36
Setting up Pager Alerts for Device Variables....37
Setting up SNMP Trap Alerts....39
SNMP Trap Destinations....39
Setting up SNMP Trap Alerts for Device Variables....39
Setting up command line alert to control a Sensorsoft Relay....41
Upgrading the firmware on your Alert Appliance....44
Accessing Sensorsoft devices on Alert with other monitoring software....44
Managing multiple Alert Appliances with RWME Software....44
Root User....45
Changing the root password....45
Recovering from a lost root password....45
Model SSA7001....45
Models SSA7004 and SSA7008....45
Backup files on Alert appliance to a remote host....47
Backup flash settings (script) file to a remote host....47
Backup log files to a remote host....47
Restore known good script backup file to Alert appliance from a remote host....48
SNMP Interface....49
Sensorsoft Alert SNMP Agent Specifications....49
Scalar and Boolean class Variables....49
Sensorsoft Alert MIB....49
Sensorsoft Alert Indexed MIB Usage....50
Setting Breach Limits on Scalar Variables....50
Setting Breach Limit on Boolean Variables....51
Setting up SNMP Trap Alerts....52
Structure of SNMP Traps from Sensorsoft Alert....53
Setting up Email Alerts through SNMP....53
Setting up Command Line Alerts through SNMP....54
Description of Alert MIB Objects....55
Security Considerations....73
Multi-Level User Access....73
Password Encryption....73
User Definable Web Server Port....73
Trouble Shooting....74
General Problems....74
View Monitor List Error Messages....75
Email Problems....76
Paging Problems....77
Getting Help....79
Limited Warranty....79
Technical Support....79
30 Day Money Back Guarantee....79

Returns 79
Appendix A - Using Dollar Variables in Messages 80
Appendix B - Controlling the SR6171J Sensorsoft Relay using Command Lines 81
Appendix C - Pager Tutorial 82
Appendix D - Modem DIP Switch Settings 84
Appendix E – Alert Serial Port Pin-outs 85
Appendix F – Using XML Output to Move Data to other Applications 86
Accessing the XML page 86
XML data organization 87
Appendix G – Setting up a Routine Email Notification within the Linux shell 88

About This Manual

This document contains information about the initial setup, routine configuration, usage and troubleshooting of Sensorsoft Alert appliance.

When other sections of this manual are referenced, *Italics* are used.

The term Sensorsoft device and its acronym SSD refer to devices that use the Sensorsoft Device Protocol.

When the phrase “the appliance” is used, it refers to Sensorsoft Alert appliance.

Some portions of this manual may only apply to model SSA7001, a single port Sensorsoft Alert appliance. Whereas, other portions may refer to no longer available multi-port Sensorsoft Alert appliances, such as models SSA7004 and SSA7008.

Glossary of Acronyms

CRC – Cyclic Redundancy Check – an algorithm for finding errors in data packets

IANA – Internet Assigned Numbers Authority

ISP – Internet Service Provider

MIB – Management Information Base – a file that describes the objects contained in an SNMP Agent

NFS – Network File System

NMS – Network Management Software

NTP – Network Time Protocol

PSP – Paging Service Provider

RWME – Remote Watchman Enterprise software

RWMC – Remote Watchman Client software

SMS – Short Message Service – defines any alphanumeric message that is sent to a paging device.

SNMP – Simple Network Management Protocol – used to monitor network traffic and devices on a TCP/IP network

SMTP – Simple Mail Transfer Protocol – used to send e-mail messages over a TCP network

SSD – SensorSoft Device – a device that incorporates the Sensorsoft Device Protocol.

SSDP – SensorSoft Device Protocol – an auto discovery protocol that allows communications between a device and a computer without any user intervention.

TAP – Telocator Alphanumeric Protocol – used to send alphanumeric messages to a pager

Overview

Sensorsoft Alert is a line of standalone, network-ready appliances that allow you to monitor remote environments through a web browser or an SNMP Network Management Station. The Sensorsoft Alert product line is available in 1, 4 and 8 port models. Serial ports on the Alert product accept the full line of Sensorsoft devices (except SS6420J/E and SS8002) that allow monitoring of temperature, humidity, flooding, power-loss and dry contacts. The advantages of Sensorsoft devices include:

- Built-in CRC algorithm checks data integrity, allowing them to be up to 1000 ft from the Alert appliance
- An auto-discovery algorithm permits plug and go operation with little user set-up required
- SSD's are powered from the Alert appliance, preventing the need for additional power supplies

In addition to Sensorsoft devices, Sensorsoft Alert also accepts third party serial devices that have Sensorsoft Plug-in support. This allows Alert to monitor a wide range of devices that have a serial (RS232) interface.

Sensorsoft Alert can be configured to issue alerts when monitored environmental conditions breach user defined limits. The following alert methods are supported:

- SNMPv1 traps
- Email messages
- SMS-TAP messages to pagers and cell phones (not available on SSA7001)
- Command line execution
- Visual alerts on the web interface

Sensorsoft Alert also has the ability to log and graph data that it collects from a device, using the built-in Sensorsoft Graphing Tool (Java applet). Existing users of Sensorsoft software such as Remote Watchman Client, SCOM Serial Communications Tool and Remote Watchman Enterprise can also monitor SSD's on the Sensorsoft Alert Appliance.

Software specifications and features

SSA7001

Max Number of Sensors or Devices	▪ 1
Supported Protocols	▪ HTTP ▪ FTP ▪ SSDP (Sensorsoft Device Protocol) ▪ DHCP ▪ DNS ▪ SNMP ▪ NFS ▪ NTP ▪ SSH/SCP ▪ SMTP ▪ SMS-TAP
Operating System	▪ Linux 2.2.14
Alerting Methods	▪ Email messages using SMTP ▪ Command line execution ▪ SNMPv1 traps
Data Logging	▪ 1600 readings for each monitored environmental variable ▪ Unlimited readings can be logged on remote NFS server
Graphing	▪ Sensorsoft Graphing Tool (SGT)
Management Options	▪ Web interface ▪ SNMP NMS (Network Management System) ▪ Sensorsoft Remote Watchman Enterprise (purchased separately) ▪ Linux shell through SSH and serial console
Data Exportation Options	▪ SNMP ▪ XML
Date/Time Keeping	▪ NTP for network or internet time synchronization
Web Interface Access Accounts	▪ Administrator (admin) ▪ Read-only User (ruser)

SSA7004 and SSA7008

Max Number of Sensors or Devices	▪ 4 for SSA7004 ▪ 8 for SSA7008
Supported Protocols	▪ HTTP ▪ FTP ▪ SSDP (Sensorsoft Device Protocol) ▪ DHCP ▪ DNS ▪ SNMP ▪ NFS ▪ NTP ▪ SSH/SCP ▪ SMTP ▪ SMS-TAP
Operating System	▪ Linux 2.2.14
Alerting Methods	▪ Email messages using SMTP ▪ SMS-TAP messaging ▪ Command line execution ▪ SNMPv1 traps
Data Logging	▪ SSA7004 - (400) readings for each monitored variable ▪ SSA7008 - (200) readings for each monitored variable ▪ Unlimited readings can be logged on remote NFS server
Graphing	▪ Sensorsoft Graphing Tool (SGT)
Management Options	▪ Web interface ▪ SNMP NMS (Network Management System) ▪ Sensorsoft Remote Watchman Enterprise (purchased separately) ▪ Linux shell through SSH and serial console
Data Exportation Options	▪ SNMP ▪ XML
Data/Time Keeping	▪ NTP for network or internet time synchronization ▪ Battery backed date and time
Web Interface Access Accounts	▪ Administrator (admin) ▪ Read-only User (ruser)

Hardware specifications

SSA7001

CPU	50 MHz MPC855T (PowerPC Dual-CPU)
Memory	32 MB RAM / 4 MB Flash
Interfaces	1 Ethernet 10/100BT on RJ45 1 RS232 Serial Port on DB-9M
Power	External Universal AC, 100-240VAC, 50/60 Hz, 5 VDC, 3 W max
Operating Temperature	50°F to 112°F (10°C to 44°C)
Storage Temperature	-40°F to 185°F (-40°C to 85°C)
Humidity	5% to 90% non-condensing
Dimensions	2.8 x 3.4 x 1.2 in (7.0 x 8.5 x 3.0 cm) (standard 35mm DIN-rail based, 4 module width)
Cover	Noryl VO 1550 base, aluminum cover
Certification	FCC Part 15, A EN55022, A

SSA7004 and SSA7008

CPU	50 MHz MPC855T (PowerPC Dual-CPU)
Memory	32 MB RAM / 4 MB Flash
Interfaces	1 Ethernet 10/100BT on RJ45 1 RS232 Serial Console on RJ45 4 RS232 Serial Ports on RJ45 (SSA7004) 8 RS232 Serial Ports on RJ45 (SSA7008)
Power	External Universal AC, 100-240VAC, 50/60 Hz, 5 VDC, 6 W max
Operating Temperature	50°F to 112°F (10°C to 44°C)
Storage Temperature	-40°F to 185°F (-40°C to 85°C)
Humidity	5% to 90% non-condensing
Dimensions	8.5 x 4.75 x 1 in (21.59 x 12.07 x 2.54 cm)
Cover	Steel enclosure
Certification	FCC Part 15, A EN55022, A

Safety Instructions

Read the following safety guideline to protect yourself and your Sensorsoft Alert Appliance.

- **DANGER!** - Do not operate your Sensorsoft Alert appliance with the cover removed.
- **DANGER!** - In order to avoid shorting out your Sensorsoft Alert appliance when disconnecting the network cable, first unplug the cable from the equipment and then from the network jack. When reconnecting a network cable to the equipment, first plug the cable into the network jack, and then into the equipment.
- **DANGER!** – Do not push any objects through the openings of the Sensorsoft Alert appliance. Doing so can cause fire or electric shock by shorting out interior components.
- **Important!** – To help protect the Sensorsoft Alert appliance from electrical power fluctuations, use a surge suppressor, line conditioner, or uninterruptible power supply.
- **Important!** – Be sure that nothing rests on the cables of the Sensorsoft Alert appliance and that they are not located where they can be stepped on or tripped over.
- **Important!** – Do not spill food or liquids on the Sensorsoft Alert appliance. If it gets wet, contact Sensorsoft.
- **Important!** – Keep your Sensorsoft Alert appliance away from heat sources and do not block cooling vents.

Working inside the Sensorsoft Alert Appliance

Do not attempt to service the Sensorsoft Alert appliance yourself, except when following instructions from Sensorsoft Technical Support personnel. In the latter case, first take the following precautions:

- Turn the Sensorsoft Alert appliance off.
- Ground yourself by touching an unpainted metal surface on the back of the equipment before touching anything inside it.

Replacing the Battery

A coin-cell battery maintains date and time information in SSA7004 and SSA7008. The SSA7001 does not have this battery, so it must use NTP to keep the date and time up-to-date.

WARNING: There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type (**3V Lithium CR2032**). Dispose of used batteries according to the manufacturer's instructions.

FCC & DOC Notice

FCC Warning Statement

This equipment generates, uses, and can radiate radio-frequency energy, and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication.

It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Canadian DOC Notice

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Alert Quick Start

This section will show you how to bring your Alert appliance up on the network. There are two different methods for accessing the Alert appliance.

The easiest method for accessing the Alert appliance is using DHCP. A new Alert appliance, from the factory, has DHCP enabled by default. This method is covered in the section, *Accessing the Alert appliance using DHCP*. The other or fail-safe method for accessing the Alert appliance is through its serial port console. This method is covered in the section, *Connecting to the Alert serial port console*.

To bring your Alert appliance up on the network work through each of the follow manual sections in the order shown here:

1. *Accessing the Alert Appliance using DHCP*
   or
   Connecting to the Alert serial port console
2. *Configure the Alert appliance's IP settings*
3. *Connect Sensorsoft device(s) to the Alert appliance*
4. *Login to the Alert web interface*

Accessing the Alert appliance using DHCP

To use this method you must have a DHCP server active on your network and a SSH client (i.e. putty) installed on your computer or workstation. This method works for a new Alert appliance or one that previously used DHCP to obtain its IP address.

1. Plug an Ethernet patch cable (i.e. P/N C2006) between your network switch, hub, or network jack and the Alert appliance's Ethernet jack.
2. Make sure that the amber Link LED (right top of Ethernet jack) on the Alert appliance is continuously illuminated. Wait up to one minute for this action if the Alert appliance is booting up. The illuminated link LED indicates that the Alert appliance is connected to a valid Ethernet network port. Otherwise check that the switch-network jack is enabled, cables are working and properly connected.
3. To find the IP address that the Alert appliance acquired, login to your DHCP server as administrator or contact your network administrator for help. A DHCP server can often be part of a file server, firewall, Internet router or Ethernet switch. Locate and note the MAC address printed on the bottom of the Alert appliance. Find this MAC address in your DHCP server's address lease or reservation list. Locate and note down the IP address that is associated (in same row) with your MAC address. This IP address is the one assigned to your Alert appliance.
4. Using a SSH client on your workstation or computer, connect to the Alert appliance using the IP address noted above. The correct port number for SSH is 22. If you are using a Windows computer you will likely have to install this SSH software. We suggest you Google "putty" a freely available SSH client.
5. Login to the Alert appliance using username: **root**, and the default root password: **sensorsoft**.
6. Proceed to section, *Configuring IP settings of the Alert Appliance* if you want to check the IP settings or set a static IP on the Alert appliance. Otherwise proceed to the next step in the Alert Quick Start procedure above (i.e. *Connect Sensorsoft device(s) to the Alert appliance*).

Connecting to the Alert serial port console

The Alert console port (DB-9M connector) is an RS232 serial interface that can be used to access the Linux shell of the Alert appliance. It is used for the purpose of configuration or recovery if you lose contact with the Alert appliance. Since this same DB-9M port is also used as the sensor port, you must carefully follow the procedure below to use it as the console port. To use this procedure you need a computer or workstation with an available RS232 serial port, a terminal program (HyperTerminal on Windows), a paper clip and the cables/adapters supplied with Alert appliance. The following procedures for connecting to your Alert console port differ depending on whether you have an SSA7001 or SSA7004/7008 model. Be sure to follow the procedure that is suitable for your Alert appliance.

Model SSA7001

To connect to your SSA7001 appliance through its console port, you first need the following items:

- A computer with a spare RS232 serial port.
- If the spare serial port on your computer is DB-9M, then you will also need the P/N C4002 adaptor. This is a gray DB-25M to DB-9F adapter that came with your Alert appliance.
- The P/N C2017 cable. This is a light blue DB-9F to DB-25F cable that came with your SSA7001 Alert appliance.

1. Make sure your Alert appliance is powered off.
2. Disconnect any device that is connected to the serial port of your Alert appliance.
3. Connect the DB-9F (female) end of the P/N C2017 cable to the serial port of your Alert appliance.
4. If the spare serial port on your computer is DB-9, then connect the other end of the P/N C2017 cable to the P/N C4002 adapter and to your computer's serial port.
5. Launch a terminal emulation program on your computer. If your computer's operating system is Windows you can use HyperTerminal located under Start > Program > Accessories. If your computer's operating system is UNIX, you can use either Kermit or Minicom.
6. Configure the terminal program parameters as shown below, and then connect.

    1. Serial Speed: 9600 bps
    2. Data Bits: 8 bits
    3. Parity: None
    4. Stop Bits: 1
    5. Flow Control: None
    6. Emulation: ANSI

7. Use a paper clip to push in the ADM button located inside a small hole on the back of the Alert appliance. Keep it pushed in as you plug in the power adapter to the Alert appliance. You can release the ADM button twenty seconds after powering on the Alert appliance, or as soon as you see some text appear on your terminal screen, whichever is first.
8. Some messages will be printed on the terminal screen as the Alert appliance boots up. When the Alert appliance finishes booting, you will see the prompt:

    [root@(none) /]#

    You are now logged in.
9. To configure the appliance's IP settings, go to section *Configuring IP Settings of the Alert Appliance*.

Models SSA7004 and SSA7008

To connect to your SSA7004 or SSA7008 appliance through its console port, you first need the following items:

- A computer with a spare serial port.
- The P/N C4003 adaptor or the P/N C4004 adaptor. Both of these adaptors came with your Alert appliance, and are gray colored. The P/N C4003 adaptor has a DB-9F connector. The P/N C4004 adaptor has DB-25F connector. Choose the one that fits the spare serial port of your computer.
- The P/N C2013 cable that came with your Alert appliance. This is a blue RJ-45 straight-through cable.

1. Make sure your Alert appliance is powered on.
2. Connect one end of the blue RJ-45 straight-through cable (P/N C2013) to the console port on the Alert appliance. The console port is located on the back of the Alert appliance, and is labeled "CONSOLE".
3. Connect the other end of the blue RJ-45 straight-through cable (P/N C2013) to the gray colored connector (P/N C4003 or C4004) labeled "Console".
4. Connect the gray colored connector to the serial port on your computer.
5. Launch a terminal emulation program on your computer. If your computer's operating system is Windows you can use HyperTerminal located under Start > Program > Accessories > Communications. If your computer's operating system is UNIX, you can use either Kermit or Minicom.
6. Configure the terminal program parameters as shown below, and then connect.
   - Serial Speed: 9600 bps
   - Data Bits: 8 bits
   - Parity: None
   - Stop Bits: 1
   - Flow Control: None
   - Emulation: ANSI
7. After you are connected, you should see a login prompt on your terminal screen. If you do not see this, press **Enter** on your keyboard a few times.
8. Login using username: **root**, and your root password. If you have never changed the root password of your Alert appliance, use the default root password: **sensorsoft.**
9. To configure the appliance's IP settings, go to section *Configuring IP Settings of the Alert Appliance*.

Configuring IP settings of the Alert Appliance

1. If you have not already done so, connect the Alert appliance's Ethernet port to the network using your own Ethernet patch cable or a P/N C2006 cable.
2. If you are continuing from the previous section such as *Accessing the Alert appliance using DHCP* or *Connecting to the Alert serial port console*, then you are already logged in and may continue to step 3. Otherwise go back to the beginning of *Alert Quick Start* section (above).
3. At the Linux shell prompt, type **wiz** and press **Enter**. This will bring up the configuration wizard. Press **Enter** to continue.

a. When prompted with the question "*Set to defaults ? (y/n)*", type **N** and press the **Enter** key.

b. You can now configure the following network settings. Ask your network administrator if you do not have this information.

- Hostname
- DHCP enabled / disabled
- System IP (DHCP disabled)
- Domain Name
- Primary DNS Server
- Gateway IP
- Network Mask (DHCP disabled)

c. When prompted with the question "*Are all these parameters correct (Y)es or (N)o*", press **N** if you want to change any of the setting you have made, otherwise press **Y**. Press the **Enter** key.

d. When prompted with the question "*Do you want to activate your configurations now? (Y/N)*", press **N** and press the **Enter** key.

e. When prompted with the question "*Do you want to save your configurations to flash (Y/N)*", press **Y** and press the **Enter** key.

4. After the appliance is finished saving the configuration to flash, the configuration wizard will automatically exit, bringing you back to the command prompt.
5. At the command prompt, type **signal_ras hup** and hit **Enter**. This will activate the new IP settings. If you are logged into the Alert appliance through Secure Shell, then you may now get disconnected.
6. If you are configuring the SSA7001 model appliance through the serial console, then you must reboot the appliance in order to restart its SNMP, web, and monitoring activities. To reboot the appliance, at the command prompt type **reboot** and press **Enter**. The appliance will now reboot, and will be back online in 1 minute. After the appliance has rebooted, disconnect the P/N C2017 cable from the appliance's serial console port.
7. Ping the Alert appliance using its IP address from a computer to verify that the new IP settings are valid and active.
8. Now proceed to the next step in the Alert Quick Start procedure above (i.e. *Connect Sensorsoft device(s) to the Alert appliance*).

Connecting Sensorsoft devices to the Alert Appliance

Sensorsoft devices that are to be monitored by Alert appliance must be physically connected to its serial port(s). Models SSA7001, SSA7004 and SSA7008 have different methods for connecting Sensorsoft devices. Follow the procedure that is suitable for your Alert appliance.

Model SSA7001

The SSA7001 appliance has one serial port with a DB-9M connector where a Sensorsoft device may be connected. This is the same connector that is used for the console.

1. Determine the model of the Sensorsoft device you are connecting to the Alert appliance. The model is printed on the plastic enclosure of the Sensorsoft device.
2. If the Sensorsoft device is the **C**-type (i.e. ST6105**C**, SM6204**C**, SS6610**C**, SM6201**C**, etc), then it has a built-in cable with a DB-9F connector at the end. Connect the cable to the SSA7001 appliance's DB-

9M port. If the Sensorsoft device is the **J**-Type (i.e. ST6105**J**, ST6154**J**, SM6204**J**, SS6610**J,** SP6400**J,** SS6402**J,** SS6201**J**), then it has an RJ45 connector. In this case, you need to use the P/N C2000 cable (RJ-45 to DB-9F). Connect the RJ45 end to the Sensorsoft device, and the DB9F end to the Alert appliance's DB9M port.

3. Now proceed to the next step in the Alert Quick Start procedure above (i.e. *Login to the Alert web interface*).

Models SSA7004 and SSA7008

The SSA7004 and SSA7008 appliances have 4 and 8 serial ports, respectively, with RJ45 connectors. These ports are physically located at the back of the appliance and are numbered starting from 1. Sensorsoft devices should not be connected anywhere else other than these numbered ports. **Do not connect any Sensorsoft device to the Ethernet port or the console port**. To connect a Sensorsoft device to the Alert appliance, follow the procedure below:

1. Determine the model of the Sensorsoft device you are connecting to the Alert appliance. The model is printed on the plastic enclosure of the Sensorsoft device.
2. If the Sensorsoft device is the SM6201CP model, then it has a built-in cable with a RJ-45 connector at the end. Connect this cable to a serial port on the Alert appliance. If the Sensorsoft device is the **J**-Type (i.e. ST6105**J**, ST6154**J**, SM6204**J**, SS6610**J,** SP6400**J,** SS6402**J,** SS6201**J**), then it has a RJ45 connector. You would need to obtain the P/N C2016 cable (RJ45 to RJ45). Connect the end labeled **SSD** to the Sensorsoft device, and the end labeled **ALERT** to a serial port on the Alert appliance.
3. Now proceed to the next step in the Alert Quick Start procedure above (i.e. *Login to the Alert web interface*).

Alert web interface

Accounts and passwords

The Sensorsoft Alert web interface uses two accounts for access rights. The first account's username is **admin** and while you are logged in with this account, you will have full rights to change all settings. The second account's username is **ruser** (read-only user) and while you are logged in with this account, you will only be able to view the "View Monitor List" page along with a limited number of other informational pages. The initial web login password for each account is **begin**. To learn how to change these passwords, refer to section *Changing Web Login Passwords*. To learn how to reset a lost web login password, refer to section *Recovering from a Lost Web Administrator Password*.

Logging into the Alert web interface

Sensorsoft Alert can be controlled through your web browser. When you login to Alert using your web browser, you will be asked to enter a username and password.

1. Determine the IP address or domain name of the Alert appliance.
2. Type this IP address (or domain name) into the Address box of your web browser, as shown in Figure 1 below, and press **Enter**
3. In the **Username** field type in **admin or ruser**, and in the **Password** field type in **begin** (the default) or the current password.
4. Click the **login** button.

Onced logged in, Sensorsoft Alert will automatically record the login event to the log file webaccess.log. To learn more about webaccess.log, please refer to section *Logging Data*.

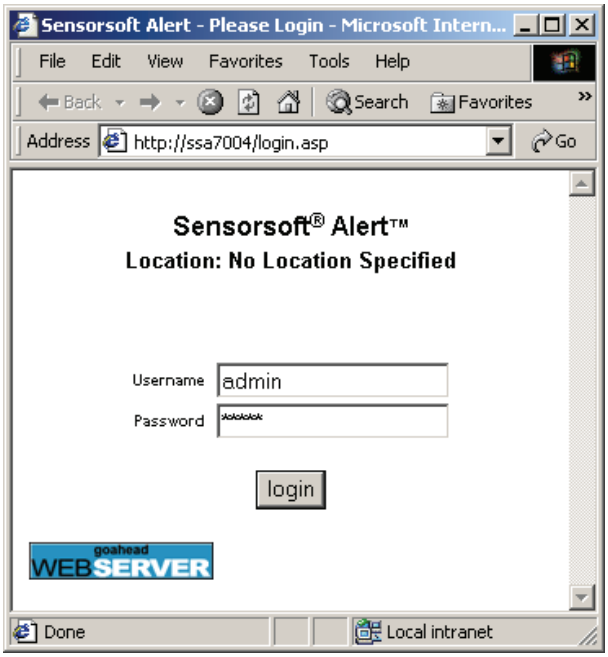


Figure 1: Alert web interface login page

Changing web login passwords:

1. Login to the Alert web interface as **admin**.
2. Click on the **Change Passwords** hyperlink located on the left side of the page. This will bring up the **Change Web Passwords** page:

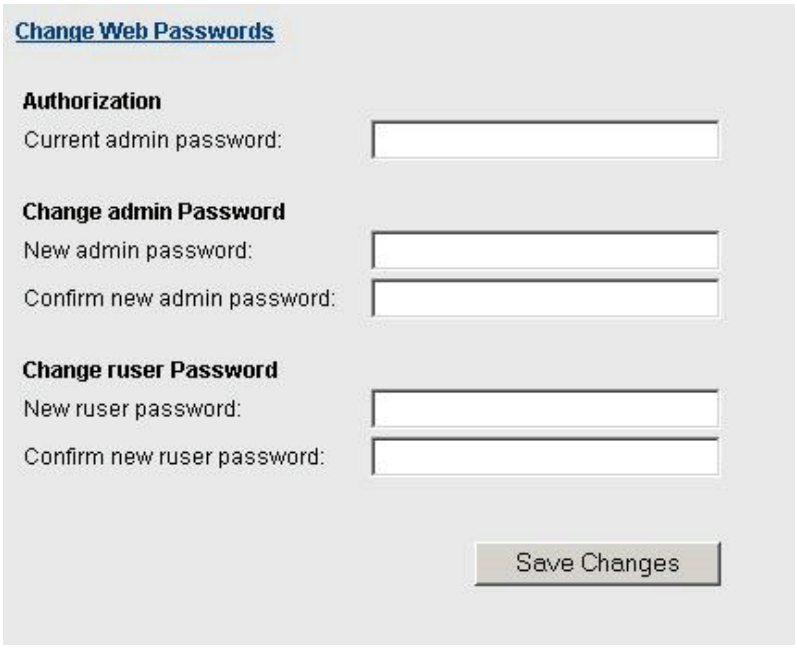


Figure 2: Change Web Passwords page

3. Enter your current admin password in the **Authorization** text field.
4. Enter the new admin password and/or new ruser password in the appropriate fields.
5. Click the **Save Changes** button.

Recovering from a lost web administrator password

The only way to recover from a lost web administrator (admin) password is to reset it to the default password: **begin**. The following procedure outlines how this is done:

1. Connect to the Sensorsoft Alert appliance though Secure Shell (SSH) or through the serial console. If the Alert appliance has not been configured with valid IP settings, then you must connect to it through the serial console (Refer to section *Connecting to the Alert Serial Console*).
2. Login as **root**.
3. At the command prompt, type **rwp** and press the **Enter** key. This will launch the Sensorsoft Web Password Reset Utility.
4. Answer **Y** to all of the questions.
5. The Alert appliance will reboot.

6. After your Alert appliance has rebooted, you will be able to login to its web interface with username: **admin** and password: **begin**. Please note that the read-only user (**ruser**) account password has also been reset to **begin**.

Setting date and time

1. Login to the Alert appliance's web interface as admin.
2. Click on the **Set Date/Time** hyperlink located on the left side of the View Monitor List page.
3. This will bring up the **Date and Time Settings** page.

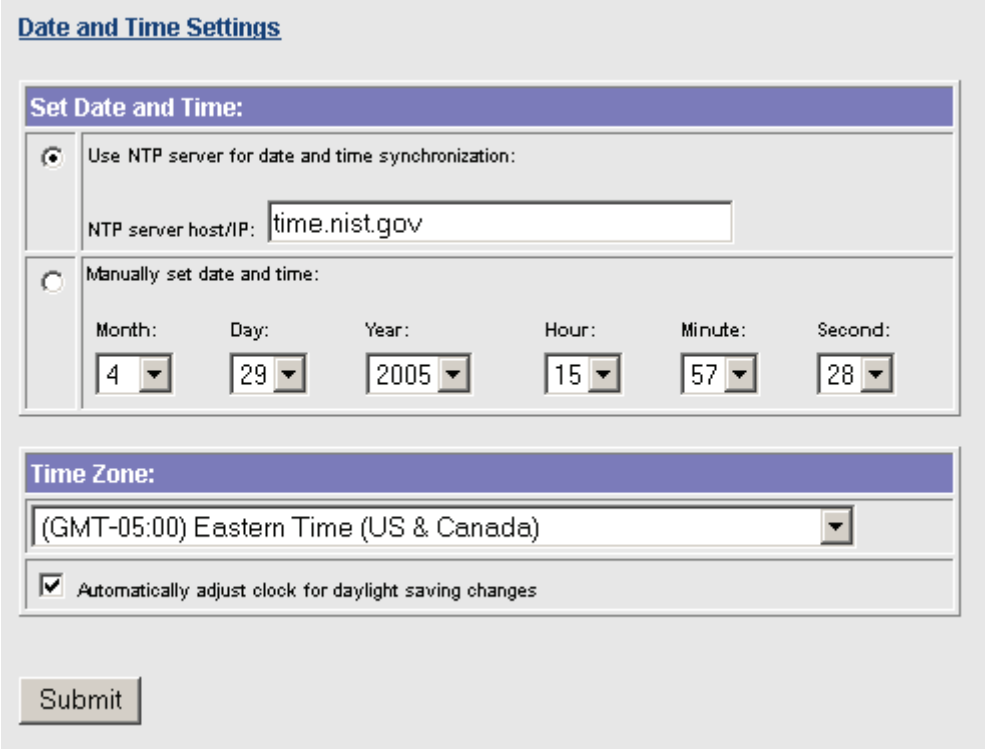


Figure 3: Setting date and time

4. You have two options for time keeping:
   a. Using an NTP Server is the recommended option. After selecting this option, you must specify an NTP server and your time zone.
   b. Manually setting the date and time is not recommended for the SSA7001 appliance, because it has no internal clock battery to keep the date and time up to date during power disconnection. The SSA7004 and SSA7008 appliances have clock batteries that will update the time during power disconnection.
5. Depending on which method you would like to use, select the appropriate radio button. If using NTP, you need to enter the NTP server host/IP in the text field provided, as well as select the time zone from the drop down box. If you would like to set the time manually, you need to set the month, day, year, hour, minute, and second from each of the drop down boxes, as well select the time zone from the drop down box. Finally, click on the **Submit** button to save your changes.

Shutting down or rebooting the Alert Appliance

IMPORTANT - It is highly recommended that you use the web interface to safely reboot or shutdown the Alert appliance. Failing to do so may cause recently saved changes to be lost.

1. Login to the Alert Appliance through the web interface as admin.
2. Click on the **Reboot/Shutdown** hyperlink located on the left side of the View Monitor List page.
3. You will see the **Reboot/Shutdown** page:

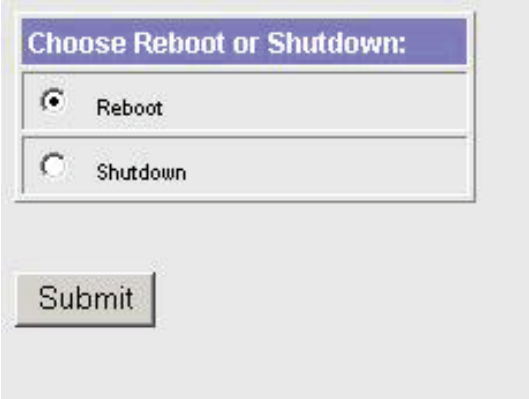


Figure 4: Reboot or shutdown through the Alert Web Interface

4. If you wish to power off the appliance, select the **Shutdown** radio button and then click the **Submit** button. Once the web interface displays that it is safe to power off the appliance, you may turn the power off. If you wish to reboot the Alert appliance, select the **Reboot** radio button and click the **Submit** button. Rebooting the appliance takes about three minutes.

Monitoring a Sensorsoft Device

To monitor a Sensorsoft device, you must first physically connect it to the Alert appliance's serial port (Please refer to section *Connecting Sensorsoft Devices to the Alert Appliance*). After this is done, follow the procedures below to configure the port for monitoring.

1. Login to the Alert web interface as **admin**.
2. Click on the **Administration** hyperlink located on the left side of the View Monitor List.
3. In the **Port Settings** table, select the **Enable Monitoring** checkbox next to the port number of the SSD.

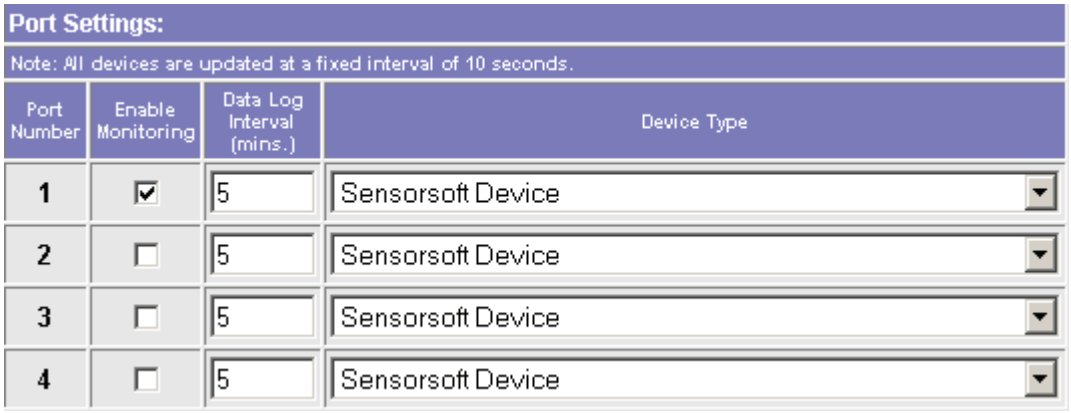


Figure 5: Configuring port settings

4. In the **Data Log Interval** field, enter the data logging interval in minutes. This defines how often the Alert appliance will record this Sensorsoft device's readings to log file.
5. In the **Device Type** dropdown list, select **Sensorsoft Device**.
6. Click on the **Save Changes** button for the change to take affect.
7. The readings from the Sensorsoft device should appear in the View Monitor List in a few seconds.

Monitoring a non-Sensorsoft Device with Plug-in Support

Your Alert appliance has the ability to monitor non-Sensorsoft serial devices using its built-in Sensorsoft Plug-in technology. A list of some non-Sensorsoft (third party) devices or instruments that are supported by Sensorsoft Alert can be found in the **Device Type** dropdown list shown in Figure 5. By default, this Device Type is set to **Sensorsoft Device**.

To monitor a third party instrument or device you need a Plug-in file that supports this device and a properly wired custom cable that connects it to the Sensorsoft Alert appliance. Once this cable is connected between your third party device and the Alert appliance, select the correct Plug-in or Device Type from the drop-down list shown in Figure 5 and click the Save Changes button. If you receive a TIME-OUT status message in the monitor list, check the following carefully:

- third party device or instrument is powered
- wiring for the custom serial cable has been verified
- plug-in or Device Type selected, matches your thirty party device or instrument
- third party device has its serial interface enabled (online)
- serial communication parameters match for third party device and the plugin_name.ini file. The plug-in always uses the default communication settings specified by the third party device manual.

To add support for other third party serial devices please contact Sensorsoft Support.

The View Monitor List Page

To access the View Monitor List page, click on the hyperlink **View Monitor List** on the left side of the Alert web interface.

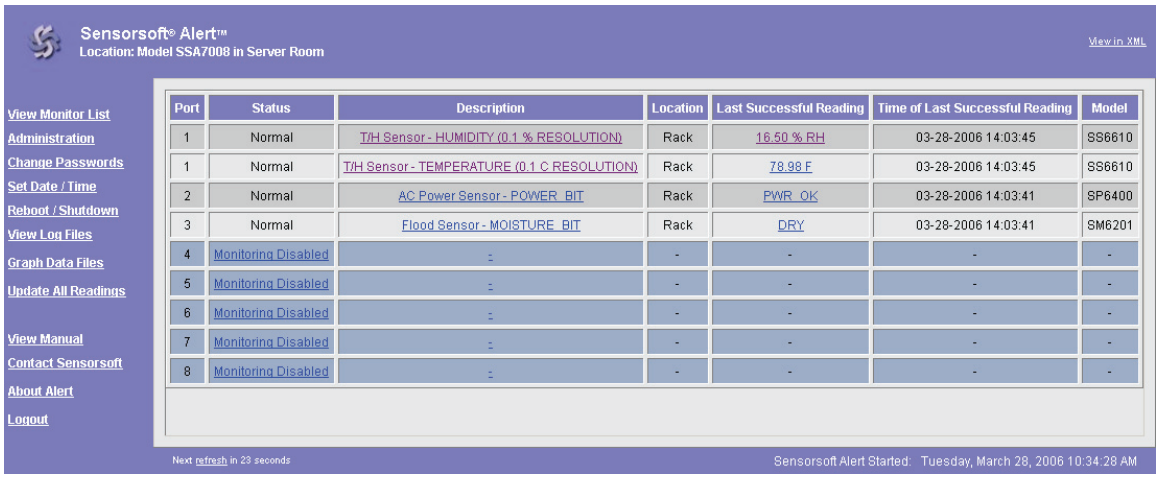

Sensorsoft® Alert™
Location: Model SSA7008 in Server Room
View in XML
View Monitor List
Administration
Change Passwords
Set Date / Time
Reboot / Shutdown
View Log Files
Graph Data Files
Update All Readings
View Manual
Contact Sensorsoft
About Alert
Logout
Port | Status | Description | Location | Last Successful Reading | Time of Last Successful Reading | Model
1 | Normal | T/H Sensor - HUMIDITY (0.1 % RESOLUTION) | Rack | 16.50 % RH | 03-28-2006 14:03:45 | SS6610
1 | Normal | T/H Sensor - TEMPERATURE (0.1 C RESOLUTION) | Rack | 78.98 F | 03-28-2006 14:03:45 | SS6610
2 | Normal | AC Power Sensor - POWER_BIT | Rack | PWR_OK | 03-28-2006 14:03:41 | SP6400
3 | Normal | Flood Sensor - MOISTURE_BIT | Rack | DRY | 03-28-2006 14:03:41 | SM6201
4 | Monitoring Disabled | - | - | - | - | -
5 | Monitoring Disabled | - | - | - | - | -
6 | Monitoring Disabled | - | - | - | - | -
7 | Monitoring Disabled | - | - | - | - | -
8 | Monitoring Disabled | - | - | - | - | -
Next refresh in 23 seconds
Sensorsoft Alert Started: Tuesday, March 28, 2006 10:34:28 AM

Figure 6: View Monitor List

This page consists of a large table that shows the overall view of all currently monitored devices connected to the Sensorsoft Alert Appliance. It serves as a system overview of all the current readings. Each row in the table displays information about a device variable that is being monitored.

This page automatically refreshes itself at a configurable interval to display the latest readings. You can manually refresh the page by clicking the **View Monitor List** hyperlink on the left side of the page

The table shown in the View Monitor List consists of the following columns:

- **Port:** This column indicates the serial port number of the Alert Appliance where each monitored device is connected. It is possible for multiple rows to have the same port number because there may be multiple variables being monitored on the same device.
- **Status:** This column indicates the status of each monitored device or variable.
- **Description:** This is a hyperlink to the Device Configuration page for each device. By clicking on this link, you can configure the alerting for a particular device. This link also allows you to specify a particular device's description and physical location.
- **Location:** This column displays each device's physical location.
- **Time of Last Successful Reading:** This column shows the time at which the last successful reading was taken from each monitored device.
- **Last Successful Reading:** This column shows the last successful reading for this particular monitored variable on the device connected to this port. Please note that if the variable reading that you want to monitor is not being displayed, refer to section *Displaying Device Variables on the View Monitor List*, which outlines how to display device variables on the View Monitor List.
- **Model:** This is the model number of the monitored device that is currently connected to this port.

Monitor List Auto-Refresh Interval

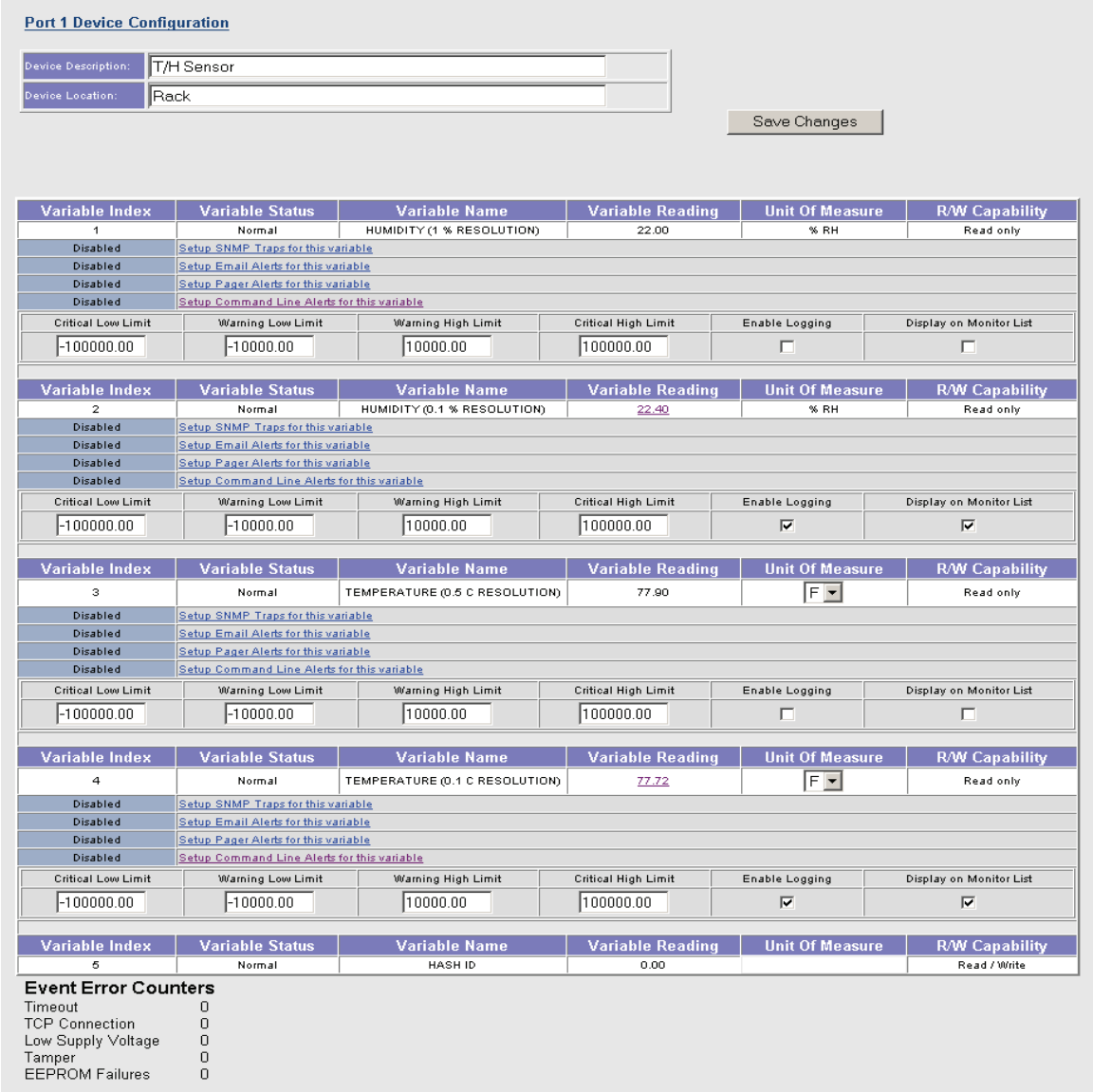
The Monitor List page (see Figure 6) auto-refreshes at a regular interval to continuously display the latest sensor readings. This interval can be configured by following the steps below:

1. Login to the Alert web interface as **admin**.
2. Click on the **Administration** hyperlink located on the left side of the View Monitor List.
3. In the **View Monitor List Display Options** table, locate the field **Monitor List Refresh Interval** and enter the refresh interval in seconds.
4. Click the **Save Changes** button at the bottom of the page.

Displaying Device Variables on the View Monitor List

Some Sensorsoft devices and Sensorsoft Plug-in supported devices can have multiple variables. For instance, the Sensorsoft SS6610J Temperature Humidity Meter has two temperature and two humidity variables. You can choose which of these variables are displayed on the View Monitor List. You may decide to display one of the temperature and one of the humidity variables. The following procedure outlines how to select variables to be displayed on the View Monitor List.

1. Determine which monitored device is of interest.
2. Login to the Sensorsoft Alert Appliance's web interface as **admin**. From the View Monitor List, click the **Description** hyperlink of the monitored device whose variables you want to add to or remove from the View Monitor List. You will see the Device Configuration page:



Port 1 Device Configuration

Device Description:	T/H Sensor
Device Location:	Rack

Save Changes

Variable Index	Variable Status	Variable Name	Variable Reading	Unit Of Measure	R/W Capability
1	Normal	HUMIDITY (1 % RESOLUTION)	22.00	% RH	Read only
Disabled	Setup SNMP Traps for this variable				
Disabled	Setup Email Alerts for this variable				
Disabled	Setup Pager Alerts for this variable				
Disabled	Setup Command Line Alerts for this variable				

Critical Low Limit	Warning Low Limit	Warning High Limit	Critical High Limit	Enable Logging	Display on Monitor List
-100000.00	-10000.00	10000.00	100000.00	☐	☐

Variable Index	Variable Status	Variable Name	Variable Reading	Unit Of Measure	R/W Capability
2	Normal	HUMIDITY (0.1 % RESOLUTION)	22.40	% RH	Read only
Disabled	Setup SNMP Traps for this variable				
Disabled	Setup Email Alerts for this variable				
Disabled	Setup Pager Alerts for this variable				
Disabled	Setup Command Line Alerts for this variable				

Critical Low Limit	Warning Low Limit	Warning High Limit	Critical High Limit	Enable Logging	Display on Monitor List
-100000.00	-10000.00	10000.00	100000.00	☑	☑

Variable Index	Variable Status	Variable Name	Variable Reading	Unit Of Measure	R/W Capability
3	Normal	TEMPERATURE (0.5 C RESOLUTION)	77.90	F	Read only
Disabled	Setup SNMP Traps for this variable				
Disabled	Setup Email Alerts for this variable				
Disabled	Setup Pager Alerts for this variable				
Disabled	Setup Command Line Alerts for this variable				

Critical Low Limit	Warning Low Limit	Warning High Limit	Critical High Limit	Enable Logging	Display on Monitor List
-100000.00	-10000.00	10000.00	100000.00	☐	☐

Variable Index	Variable Status	Variable Name	Variable Reading	Unit Of Measure	R/W Capability
4	Normal	TEMPERATURE (0.1 C RESOLUTION)	77.72	F	Read only
Disabled	Setup SNMP Traps for this variable				
Disabled	Setup Email Alerts for this variable				
Disabled	Setup Pager Alerts for this variable				
Disabled	Setup Command Line Alerts for this variable				

Critical Low Limit	Warning Low Limit	Warning High Limit	Critical High Limit	Enable Logging	Display on Monitor List
-100000.00	-10000.00	10000.00	100000.00	☑	☑

Variable Index	Variable Status	Variable Name	Variable Reading	Unit Of Measure	R/W Capability
5	Normal	HASH ID	0.00		Read / Write

Event Error Counters

Timeout	0
TCP Connection	0
Low Supply Voltage	0
Tamper	0
EEPROM Failures	0

Figure 7: Device Configuration Page

3. Figure 7 above shows the Device Configuration page for a SS6610J Sensorsoft Temperature Humidity Meter. It has a total of 5 variables. You can select which ones you would like to display on the View Monitor List by checking the **Display on Monitor List** checkbox for that particular variable. In Figure 7, we have selected one humidity variable (HUMIDITY 0.1% RESOLUTION) as well as one temperature variable (TEMPERATURE 0.1C RESOLUTION) to be displayed on the View Monitor List.
4. Once you have selected the appropriate checkboxes, click the **Save Changes** button.

Logging Variable Readings to Data Log File

By default, variable readings are logged locally on the Alert appliance. The SSA7001 model can store the most recent 1600 log entries for each variable; the SSA7004 model can store the most recent 400 log

entries for each variable; the SSA7008 model can store the most recent 200 log entries for each variable. You can also configure Alert to record log files on a remote server using NFS (Network File System). By recording log files on an NFS server, there will be no limit on the number of entries stored in the log files. To learn more about NFS logging, please see the section *Logging Data on a NFS Server*.

In Alert Firmware Image build 12 (Software Version 1.0.74) or higher, the logging and sensor update intervals are now separate. With this enhancement, the sensor update rate is fixed at once every 10 seconds to ensure quick detection of possible breach conditions, while the logging interval for each variable can be configured. Users can configure this interval to increase the log files' time span. For example, it you set the logging interval to 9 minutes on a SSA7001, the appliance will store readings that span the last 10 days as shown by the following calculation:

9 min x 1600 readings = 14400 min = 240 hours = **10 days**

The following formula will calculate the logging interval required to achieve a specific span of time:

Logging interval = desired span in minutes ÷ log entry limit

where log entry limit is 1600 for SSA7001, 400 for SSA7004, and 200 for SSA7008.

To configure the logging interval for a particular Sensorsoft device use the following procedure and refer to Figure 7a below:

1. Login to the Alert web interface as **admin**.
2. Click on the **Administration** hyperlink located on the left side of the Monitor List.
3. In the **Port Settings** table, locate the port number of the target Sensorsoft device, and then set the corresponding **Data Log Interval** to the desired number of minutes.

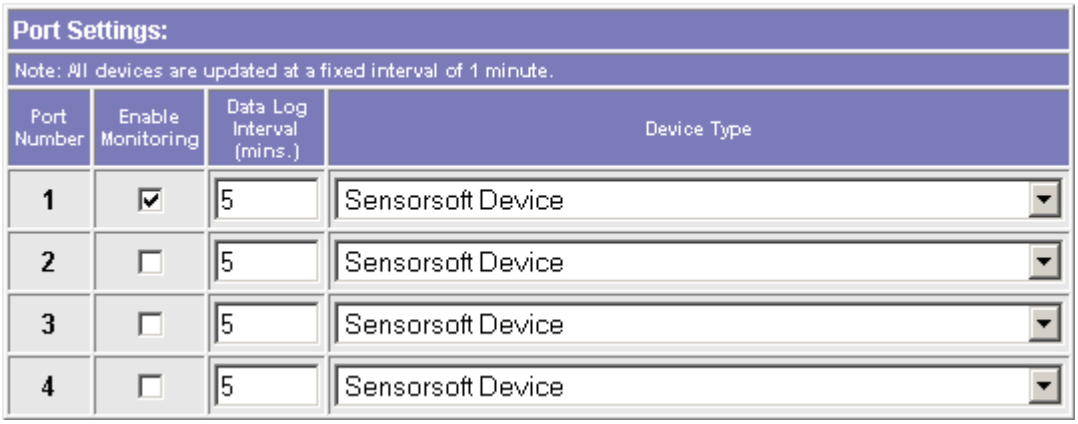


Figure 7a: Configure Data Log Interval

To enable logging for a particular variable, follow the procedures below:

1. Login to the Alert web interface as **admin**.
2. From the View Monitor List, click on the **Description** hyperlink of the device whose readings you would like to log to a file.
3. This will bring up the device configuration page for that particular device.
4. Select a variable to log by clicking on the appropriate **Enable Logging** checkbox as shown in Figure 8 below:

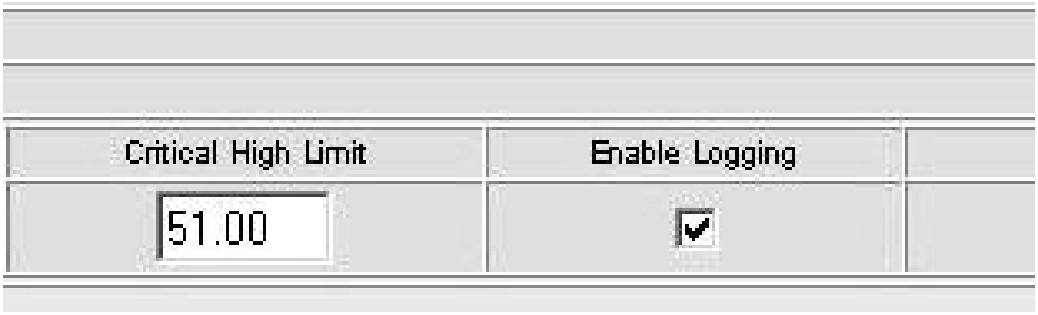


Figure 8: Enabling logging of variable readings

5. Click on the **Save Changes** button**.**

Logging Data

Sensorsoft Alert records two types of log files. Data files contain readings collected from Sensorsoft devices. This information is suitable for graphing and viewing in textual format. Status and error logs contain information collect about the status of Sensorsoft Alert and errors encountered. This information is only suitable for viewing in textual format and cannot be graphed. Both of these log files are recorded in text delimited format with date and time stamps.

Status and Error Logs

Sensorsoft Alert records the following status and error logs:

1. alertd.log: Contains systems messages and errors.
2. webaccess.log Contains web server events for user login, logout, and failed login. This log file can be viewed from the admin account only.
3. snmp.log: Contains SNMP trap alerts.
4. smtp.log: Contains email alerts that have been sent.
5. pager.log: Contains pager alerts that have been sent.
6. commandline.log: Contains command line alerts that have been executed.

By default, the above log files are recorded locally on the Alert appliance, and will contain only the most recent 200 entries. You can also configure Alert to record log files on a remote server using NFS (Network File System). By recording log files on an NFS server, there will be no limit on the number of entries stored in the log files. To learn more about NFS logging, please see the section *Logging Data on a NFS Server*.

Data file Naming Convention

Sensorsoft Alert names data files to be unique. All data log files are named in the format **_PortX_VarY.log**, where **X** is the port number and **Y** is the variable number. You will need to know what port the monitored device is connected to and the variable index on the device. This can be determined from the device configuration page of the device in question.

The following are examples of data file names:

_Port01_Var1.log

_Port08_Var4.log

Graphing data files

The data logged by Sensorsoft Alert can be graphed using the integrated Sensorsoft Graphing Tool (SGT) applet software.

There are two methods to graph data files:

a) The easiest way to graph a data file is to click on the variable's reading (hyperlink) in the Monitor List page. This will launch SGT in a separate browser window and offer a series that can be graphed. You will only be able to do this, if Alert is logging the data for this variable.

b) If the variable that you want to graph is NOT displayed on the Monitor List page, then it can be graphed by clicking the hyperlink entitled **Graph Data Files** on the left-hand side bar. This will launch SGT in a separate browser window where you can select the name of data file to graph. Log files that contain error or alerting information cannot be graphed.

For information on how to use the Sensorsoft Graphing Tool (SGT), see the Sensorsoft Graphing Tool User Manual. This can be viewed from the View Manual button on the SGT web interface.

Viewing log files

There are two methods we suggest for viewing data or log files:

a) The easiest way to view a data file is to hover your mouse pointer over the variable's reading (hyperlink) in the Monitor List page. A menu will then be displayed, where you can select the **View Data File** option. The data file will then be displayed in text format in your browser window. You will only be able to do this, if the Alert appliance is logging the data for this variable.

b) If the variable is NOT displayed on the Monitor List page, or it's an error/status log, then it can be viewed by clicking the hyperlink entitled **View Log Files** on the left side of the web page. This will display all log files available where you can select the name of the file you wish to view.

Logging Data on a NFS Server

By default, log files are recorded on the Alert appliance. The limitations of recording log files on the Alert appliance are that only a limited number of records are possible and that these are lost after a reboot or shutdown. To overcome these limitations, you can configure Alert to record log files on a remote NFS (Network File System) server. By using NFS the number of records stored can be very large or at least limited only by the size of the hard disk on the NFS server. The Alert appliance (client) does this by requesting the use of a large disk (called mounting) on a host NFS server where it will then read and write its log files. A server that supports NFS is mandatory for this feature to work. Not all servers support NFS. Most UNIX and Linux servers do offer NFS services. Please refer to your file server documentation to determine if it offers NFS server capability and the manner in which it is configured to allow permissions for the Alert appliance.

To configure the NFS server to give permissions to the Alert appliance you must do the following:

- create the directory path on the NFS server where you want the Alert log files stored
- explicitly reference the DNS name or IP address of the Alert appliance
- explicitly reference the above directory path you are permitting the Alert appliance to use

- allow the Alert appliance read/write privileges to this directory

The following example shows how to modify the /etc/exports file on a UNIX or Linux NFS server. This example allows the Alert appliance (172.17.2.100) to have read and write privileges (rw) to a directory named (/mnt/alert) on the NFS server:

```
/mnt/alert      172.17.2.100(rw,no_root_squash)
```

After making changes to the /etc/exports file on the NFS server you must restart the NFS service for the changes to take effect.

To configure the Alert appliance for recording log files on a NFS server, follow the steps below and refer to Figure 8a below:

1. Login to the Alert web interface as **admin**.
2. Click on the **Administration** hyperlink located on the left side of the Monitor List.
3. Scroll down to the table **Logging Settings** and click the checkbox Log Data to NFS Server.
4. In the field **NFS Server IP or Host Name**, enter the IP address or host name of the remote NFS server.
5. In the field **NFS Server Volume Path**, enter the existing directory path on the NFS server that Alert has permission to record its log files (e.g. /mnt/alert). Before proceeding, insure that the NFS server has this directory path and that the Alert appliance is named and permitted read/write privileges.
6. Click the **Save Changes** button at the bottom of the page.

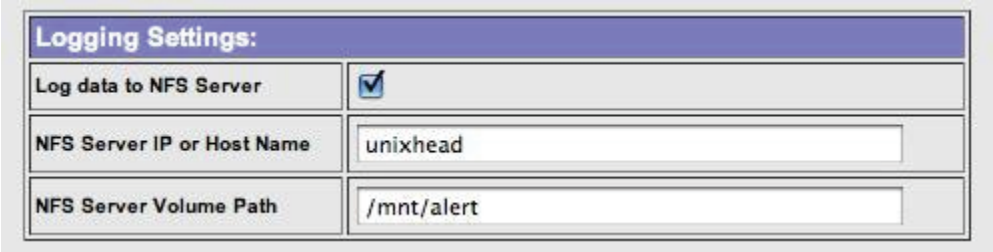


Figure 8a: NFS Logging Settings

Setting up Alerts

Your Alert appliance has the ability to alert you when a variable reading is in a warning or critical state. There are two parts to setting up alerts for a particular variable. The first part is to specify at what values is a particular variable in warning or critical state. The second part is to specify what alert actions should be taken when a particular variable is in those states.

For example, you can specify that a temperature variable is in critical state if it exceeds 35^{o}C, and you may want your Alert appliance to page or email you when the variable goes into that state.

The two types of variables on Sensorsoft devices and Sensorsoft Plug-in supported devices are scalar and Boolean. Scalar variables represent qualities such as temperature and humidity. Scalar variables take on numerical values such as 73^{o}F or 25 %RH. Boolean variables represent logical values such as Power (FAIL/OK), Flooding (WET/DRY), Relay (ON/OFF) and Input Contact (OPEN/CLOSED).

A scalar variable can be in one of 5 possible states:

1. **Breach of Critical High Limit**
   A scalar variable goes into this state when its value becomes greater than or equal to the Critical High Limit.
2. **Breach of Warning High Limit**
   A scalar variable goes into this state when its value becomes greater than or equal to the Warning High Limit but less than the Critical High Limit.
3. **Breach of Warning Low Limit**
   A scalar variable goes into this state when its value becomes less than or equal to the Warning Low Limit.
4. **Breach of Critical Low Limit**
   A scalar variable goes into this state when its value becomes less than or equal to the Critical Low Limit.
5. **Normal**
   A scalar variable is in this state when its value is less than the Warning High Limit and greater than the Warning Low limit.

A Boolean variable can be in one of 2 possible states:

1. **Breach of Boolean Critical State**
   A Boolean variable goes into this state when its value is equal to the Boolean Critical Value.
2. **Normal**
   A scalar variable is in this state when its value is not equal to the Boolean Critical Value.

Setting up Alerting Limits for Device Variables

1. Login to the Alert web interface as **admin**.
2. On the View Monitor List page, click on the **Description** hyperlink for the monitored device of interest.
3. On the **Device Configuration** page, you will see a table that lists information about every variable on this monitored device. Locate the variable that you would like to set alerting limits for. If the variable of interest is a scalar variable, then you will need to set the alerting limits in the Critical Low Limit field, Warning Low Limit field, Warning High Limit field, and Critical High Limit field as shown in Figure 8. These values should be set in a rising order from Critical Low Limit to Critical High Limit.

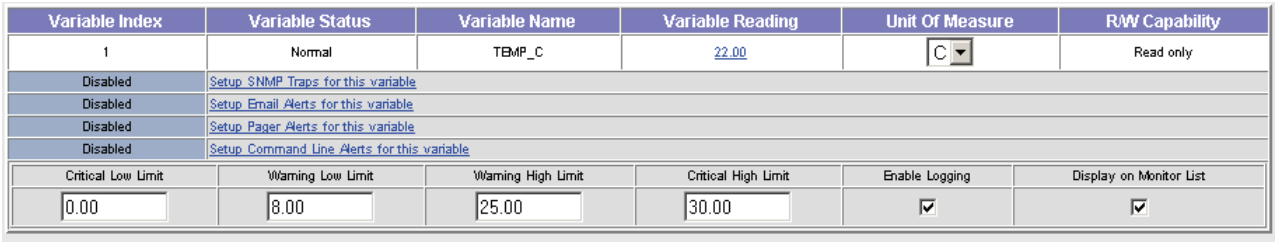


Figure 8b: Setting alerting limits for a scalar variable

If the variable is Boolean, you can be alerted when its value is equal to the Boolean Critical Value. Set the Boolean Critical Value by selecting it from the **Boolean Critical State** list-box shown below.

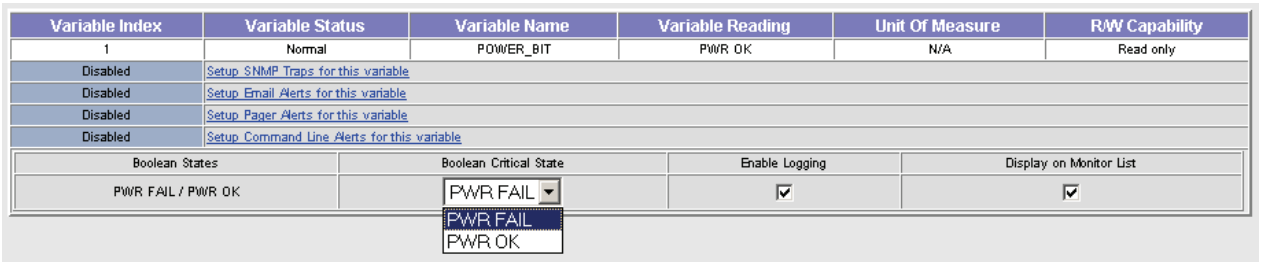


Figure 8c: Setting Boolean Critical State for a Boolean Variable

4. Click the **Save Changes** button. You are now ready to setup the individual alerting methods (e.g. Email, SMS Page, SNMP Trap and Command Lines).

Setting up Email Alerts

Email alerts are useful if you require a variety of people within or outside of your organization to be alerted to potential problems. This type of alert can be sent to anyone with an e-mail address. In some cases, your paging provider may provide an e-mail address for your personal paging device. Please contact your paging provider for more details. To send alerts via email you will need to have access to an SMTP mail server that will accept your requests. Sensorsoft Alert does not provide any form of SMTP authentication.

SMTP Settings

For your Alert appliance to send alerts via email, you must properly configure the SMTP settings.

1. Login to the Alert web interface as **admin**.
2. Go to the Administration page by clicking on the **Administration** hyperlink located on the left side of the web page. The General Administration Settings page will come up. In the middle of the page, you will see the **SMTP Settings** table:

Figure 10: SMTP Settings on the Administration Page

You must enter at least one valid SMTP server address to be used for sending emails. When sending out an Email alert, your Alert appliance will attempt to use the Primary SMTP Server first. If this attempt fails, it would then try the Secondary SMTP Server. The Sender Address will indicate to the recipient(s) who the Email is from. Please note that most SMTP servers require the Sender Address to be a valid email address or else the email will NOT be sent.

3. After these fields are set, click the **Save Changes** button.

Setting up Email Alerts for Device Variables

1. Go to the **Device Configuration** page for the monitored device of interest. To get to this page, first click on the **View Monitor List** hyperlink on the left side of the web page. From the View Monitor List page, click on the **Description** hyperlink for the monitored device of interest.
2. From the **Device Configuration** page, click on the **Setup Email Alerts for this variable** hyperlink for the device variable of interest. This will take you to the Email Setup page of the variable for which to setup Email alerts.
3. The following table (Figure 11) will come up for scalar variables (e.g. temperature or humidity) on the Email Configuration page:

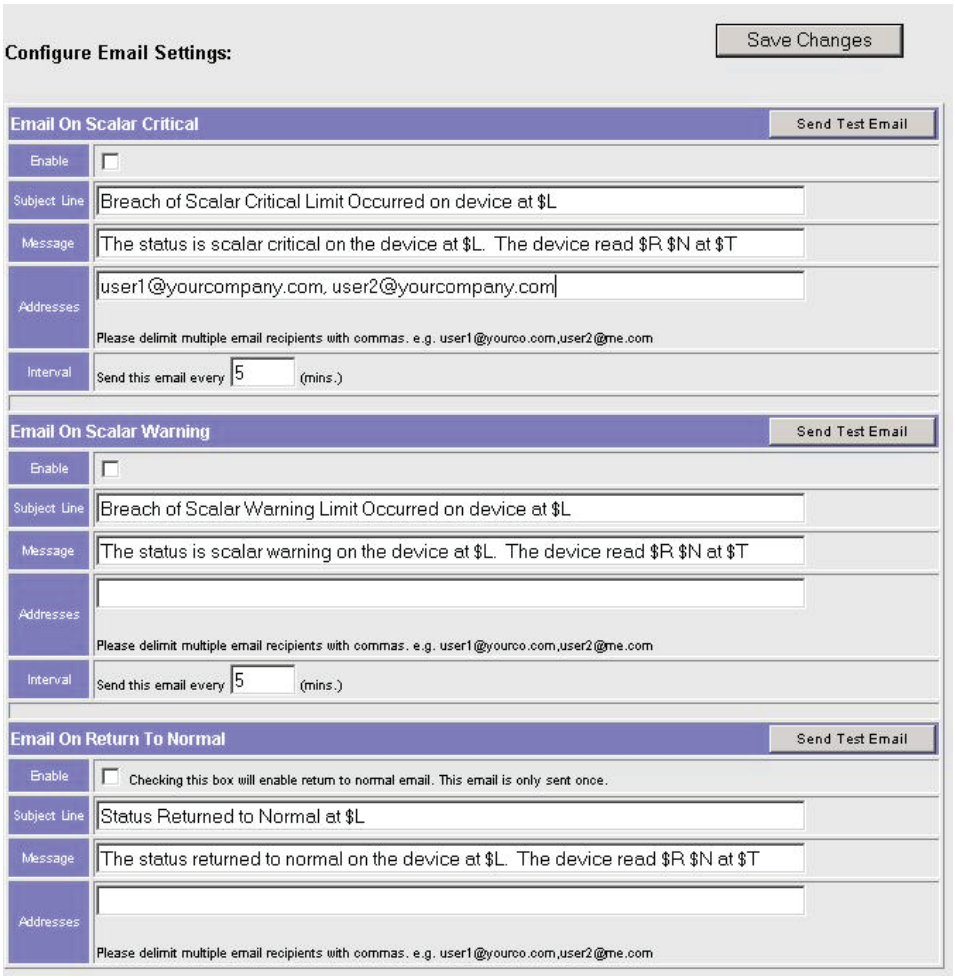

Configure Email Settings:
Save Changes
Email On Scalar Critical
Send Test Email
Enable
Subject Line
Breach of Scalar Critical Limit Occurred on device at $L
Message
The status is scalar critical on the device at $L. The device read $R $N at $T
Addresses
user1@yourcompany.com, user2@yourcompany.com
Please delimit multiple email recipients with commas. e.g. user1@yourco.com,user2@me.com
Interval
Send this email every 5 (mins.)
Email On Scalar Warning
Send Test Email
Enable
Subject Line
Breach of Scalar Warning Limit Occurred on device at $L
Message
The status is scalar warning on the device at $L. The device read $R $N at $T
Addresses
Please delimit multiple email recipients with commas. e.g. user1@yourco.com,user2@me.com
Interval
Send this email every 5 (mins.)
Email On Return To Normal
Send Test Email
Enable
Checking this box will enable return to normal email. This email is only sent once.
Subject Line
Status Returned to Normal at $L
Message
The status returned to normal on the device at $L. The device read $R $N at $T
Addresses
Please delimit multiple email recipients with commas. e.g. user1@yourco.com,user2@me.com

Figure 11: Configuring Email Alerts for a Scalar Variable

Notice that for a scalar variable, you can configure email alerts to be sent in the following alert states:

- Email on Scalar Critical – The email that will be sent when the variable reading is less than the scalar critical low limit or greater than the scalar critical high limit.
- Email on Scalar Warning – The email that will be sent when the variable reading is less than the scalar warning low limit or greater than the scalar warning high limit.
- Email on Return to Normal. – The email that will be sent when the variable reading returns to normal after breaching any limit.

For a Boolean variable, you can configure email alerts to be sent in the following alert states:

- Email on Boolean Critical – The email that will be sent when the variable reading is in the Boolean critical state.
- Email on Return to Normal. – The email that will be sent when the variable reading returns from Boolean critical state to normal state.

4. For each email alert that you would like to enable, check the corresponding **Enable** checkbox.
5. In each **Subject Line** field, specify the email subject for the corresponding alert condition. You may want to use dollar variables (e.g. $L, $R) to bind live information such as the current reading into your message. This is described in *Appendix A*.

6. In each **Message** field, specify the email message to be sent for the corresponding alert condition. You may want to use dollar variables (e.g. $L, $R) to bind live information such as the current reading into your message. This is described in *Appendix A*.
7. In each **Interval** field, specify the email interval for the corresponding breach condition. As long as the variable is in a particular breach condition, email alerts will be repeatedly sent at the interval corresponding to the breach condition.
8. In each **Addresses** field, specify the recipient email addresses for the corresponding alert condition.
9. When finished, click the **Save Changes** button.
10. It is highly recommended that you test all of your Email alerts to ensure that they are properly setup. You can test each Email alert by clicking on its **Send Test Email** button.

Setting up Pager Alerts

Paging allows people to be alerted when they are not near a computer. They can receive alerts using a pager or a cell phone with text messaging. This section outlines how to use an external modem to send pager alerts. The advantage of using a modem is that it does not rely on network access to deliver messages, and therefore provides an out-of-band method of message delivery. **Pager alerts are available only on SSA7004 and SSA7008 appliances.**

Connecting a Modem to the Alert Appliance

Sensorsoft Alert supports the following types of modems:

- Hayes
- Older Hayes
- US Robotics Sportster
- US Robotics Sportster Voice 56K
- US Robotics Courier V.Everything

Refer to your modem's documentation to find out your modem's type. The external modem must be connected to one of your Alert appliance's serial ports. These ports are located on the back of the appliance and are numbered starting from 1. You can attach the modem to any one of these ports using the supplied cable (P/N C2018, gray, DB-25M to RJ-45).

Paging Settings

To allow Sensorsoft Alert to send alerts via paging, you must properly configure the paging settings.

1. Login to the Alert web interface as **admin**.
2. Go to the Administration page by clicking on the **Administration** hyperlink located on the left side of the page. The General Administration Settings page will come up. On this page, you will see the **Paging Settings** table:

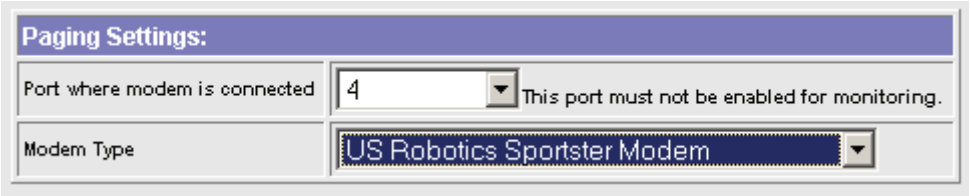


Figure 12: Paging Settings on the Administration Page

3. Select the port where the modem connected.
4. Select the correct modem type.
5. Make sure this port is NOT being monitored, by clearing the **Enable Monitoring** checkbox in the **Port Settings** table located at the top of the page.
6. Click the **Save Changes** button.

Setting up Pager Alerts for Device Variables

1. Go to the **Device Configuration** page for the monitored device of interest. To get to this page, first click on the **View Monitor List** hyperlink on the left side of the web page. From the View Monitor List page, click on the **Description** hyperlink for the monitored device of interest.
2. From the **Device Configuration** page, click on the **Setup Pager Alerts for this variable** hyperlink for the device variable of interest. This will take you to the Pager Setup page of the variable for which to setup Pager alerts.
3. On the Pager Setup page, you will see the following table in the upper right corner:

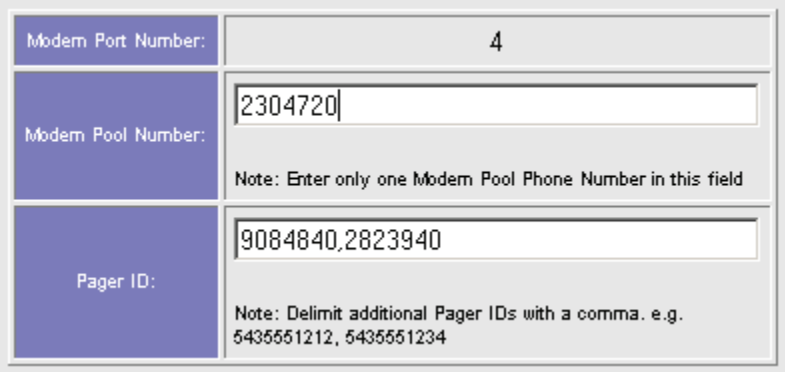

Modem Port Number:
4
Modem Pool Number:
2304720
Note: Enter only one Modem Pool Phone Number in this field
Pager ID:
9084840,2823940
Note: Delimit additional Pager IDs with a comma. e.g. 5435551212, 5435551234

Figure 13: Setting pager recipient information on the Paging Alert Configuration page

Enter the modem pool number of the paging service provider in the **Modem Pool Number** Field. There should be only one number in this field. Then, enter the recipient pager IDs in the **Pager ID** field. Multiple pager IDs must be delimited by commas.

4. If the selected device variable is a scalar variable (e.g. temperature or humidity), you will see the table shown in Figure 14 on the Pager Setup page.

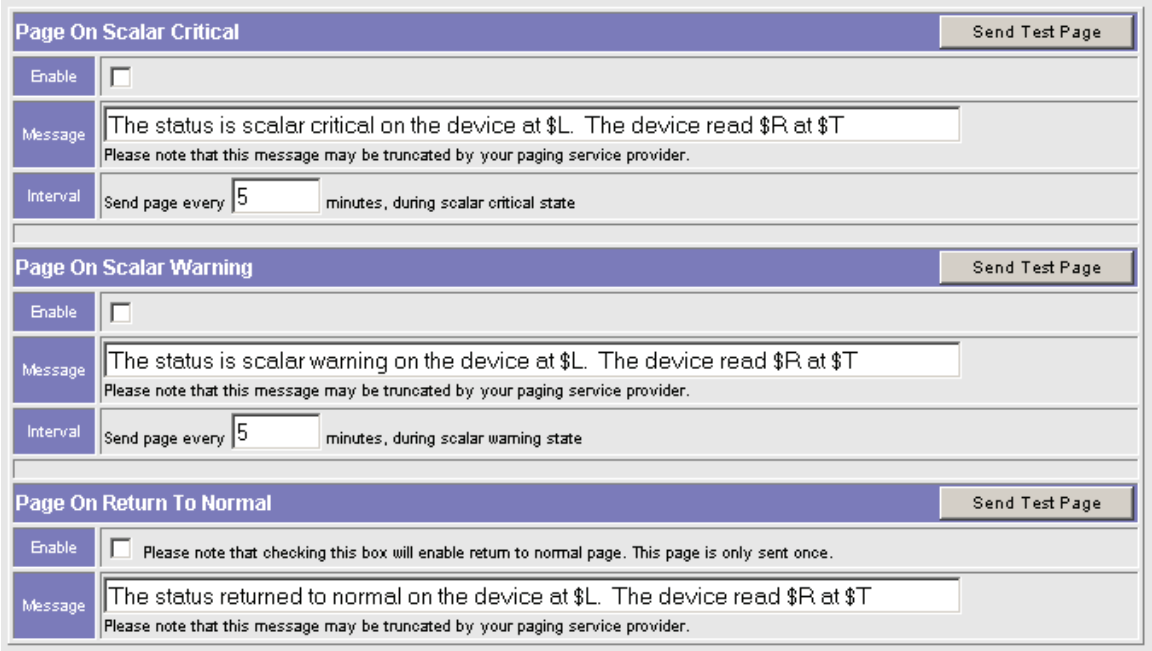

Page On Scalar Critical
Send Test Page
Enable
Message
The status is scalar critical on the device at $L. The device read $R at $T
Please note that this message may be truncated by your paging service provider.
Interval
Send page every 5 minutes, during scalar critical state
Page On Scalar Warning
Send Test Page
Enable
Message
The status is scalar warning on the device at $L. The device read $R at $T
Please note that this message may be truncated by your paging service provider.
Interval
Send page every 5 minutes, during scalar warning state
Page On Return To Normal
Send Test Page
Enable
Please note that checking this box will enable return to normal page. This page is only sent once.
Message
The status returned to normal on the device at $L. The device read $R at $T
Please note that this message may be truncated by your paging service provider.

Figure 14: Configuring pager alerts for a scalar variable

Notice that for a scalar variable, you can configure pager alerts to be sent in the following alert states:

- Page on Scalar Critical – The page that will be sent when the variable reading breaches the scalar critical low limit or the scalar critical high limit.
- Page on Scalar Warning – The page that will be sent when the variable reading breaches the scalar warning low limit or the scalar warning high limit.
- Page on Return to Normal. – The page that will be sent when the variable reading returns to normal after exceeding breach limits.

For a Boolean variable, you can configure pager alerts to be sent in the following alert states:

- Page on Boolean Critical – The page that will be sent when the variable reading is in the Boolean critical state.
- Page on Return to Normal. – The page that will be sent when the variable reading returns from Boolean critical state to normal state.

5. For each pager alert that you would like to enable, check the corresponding **Enable** checkbox.
6. In each **Message** field, specify the pager message to be sent for the corresponding alert condition. You may want to use dollar variables (e.g. $L, $R) to bind live information such as the current reading into your message. This is described in *Appendix A*.
7. In each **Interval** field, specify the paging interval for the corresponding breach condition. As long as the variable is in a particular breach condition, pager alerts will be repeatedly sent at the interval corresponding to the breach condition.
8. When you are finished, click the **Save Changes** button.
9. It is highly recommended that you test all of your pager alerts to ensure that they are properly setup. You can test each pager alert by clicking on its **Send Test Page** button. It is important to note that most SMS providers impose a maximum limit on the number of characters that a message may contain, and will truncate the message to fit the maximum length. It is therefore important to test each message to ensure it does not exceed the maximum allowed length.

Setting up SNMP Trap Alerts

SNMP trap alerts are suitable for users who need to manage their Alert appliance through SNMP. To receive SNMP trap alerts, you must have one or more NMS (Network Management Station) with the ability to receive traps.

SNMP Trap Destinations

To allow your Alert appliance to send SNMP trap alerts, you must set the SNMP trap destination IP addresses and SNMP trap destination commappliances. A trap destination is typically a computer that is running network management software. You can set a maximum of two trap destination IP addresses. The same trap destination will be used for the SNMP trap alerting of all variables on all monitored devices.

1. Login to the Alert web interface as **admin**.
2. Go to the Administration page by clicking on the **Administration** hyperlink located on the left side of the page. The General Administration Settings page will come up. On this page, you will see the **SNMP Settings** table:

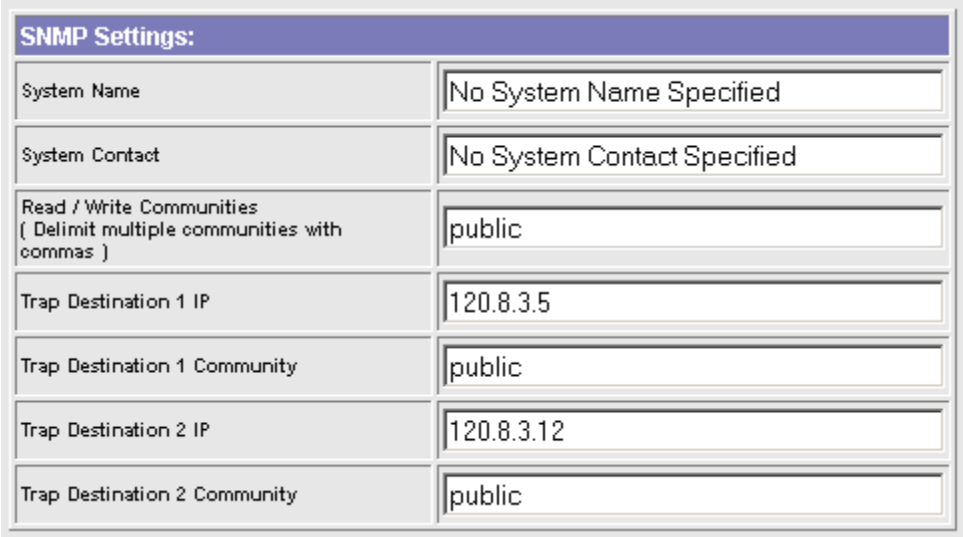


Figure 15: SNMP Settings on the Administration Page

In the fields **Trap Destination 1 IP** and **Trap Destination 2 IP**, enter the trap destination IP addresses.

3. Click the S**ave Changes** button.

Setting up SNMP Trap Alerts for Device Variables

1. Go to the **Device Configuration** page for the monitored device of interest. To get to this page, first click on the **View Monitor List** hyperlink on the left side of the web page. From the View Monitor List page, click on the **Description** hyperlink for the monitored device of interest.

2. From the **Device Configuration** page, click on the **Setup SNMP Traps for this variable** hyperlink for the device variable of interest. This will take you to the Trap Setup page of the variable for which to setup SNMP Trap alerts.
3. If the selected device variable is a scalar variable (e.g. temperature or humidity), you will see the following table on the Pager Setup page:

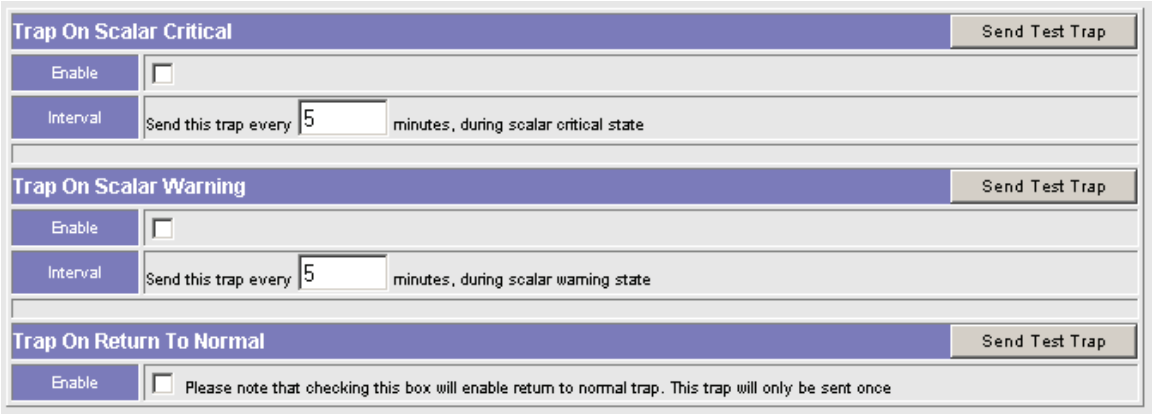

Trap On Scalar Critical
Send Test Trap
Enable
Interval
Send this trap every 5 minutes, during scalar critical state
Trap On Scalar Warning
Send Test Trap
Enable
Interval
Send this trap every 5 minutes, during scalar warning state
Trap On Return To Normal
Send Test Trap
Enable
Please note that checking this box will enable return to normal trap. This trap will only be sent once

Figure 16: Configuring Trap Alerts for a Scalar Variable

Notice that for a scalar variable, you can configure trap alerts to be sent in the following alert states:

- Trap on Scalar Critical – The trap that will be sent when the variable reading breaches the scalar critical low limit or the scalar critical high limit.
- Trap on Scalar Warning – The trap that will be sent when the variable reading breaches the scalar warning low limit or the scalar warning high limit.
- Trap on Return to Normal. – The trap that will be sent when the variable reading returns to normal after exceeding breach limits.

For a Boolean variable, you can configure trap alerts to be sent in the following alert states:

- Trap on Boolean Critical – The trap that will be sent when the variable reading is in the Boolean critical state.
- Trap on Return to Normal. – The trap that will be sent when the variable reading returns from Boolean critical state to normal state.

4. For each trap alert that you would like to enable, check the corresponding **Enable** checkbox.
5. In each **Interval** field, specify the trap interval for the corresponding breach condition. As long as the variable is in a particular breach condition, pager alerts will be repeatedly sent at the interval corresponding to the breach condition.
6. When you are finished, click the **Save Changes** button.
7. It is highly recommended that you test all of your trap alerts to ensure that they are properly setup. You can test each trap alert by clicking on its **Send Test Trap** button.

Setting up command line alert to control a Sensorsoft Relay

A Sensorsoft Relay can be controlled to turn ON or OFF when a variable reading breaches a user-defined limit. One potential application is to have a relay turn on an air conditioning appliance or audio alarm. A relay can be controlled through the use of command line alert as described below:

1. Connect a SR6171J Sensorsoft Relay to a spare serial port on the back of the Alert appliance using a C2016 cable. Ensure that the SR6171J is powered by an AC/DC adaptor (9VDC, 500 mA).
2. Login to the Alert web interface as **admin**.
3. Go to the **Administration** page and make sure the port that the relay is connected to is not being monitored.
3. Go to the **Device Configuration** page for the monitored device of interest. To get to this page, first click on the **View Monitor List** hyperlink on the left side of the web page. From the View Monitor List page, click on the **Description** hyperlink for the monitored device of interest.
4. From the **Device Configuration** page, click on the **Setup Command Line Alerts for this variable** hyperlink for the device variable of interest. This will take you to the Command Line Setup page of the variable for which to setup Command Line alerts.
5. The following Command Line alerts configuration page will come up:

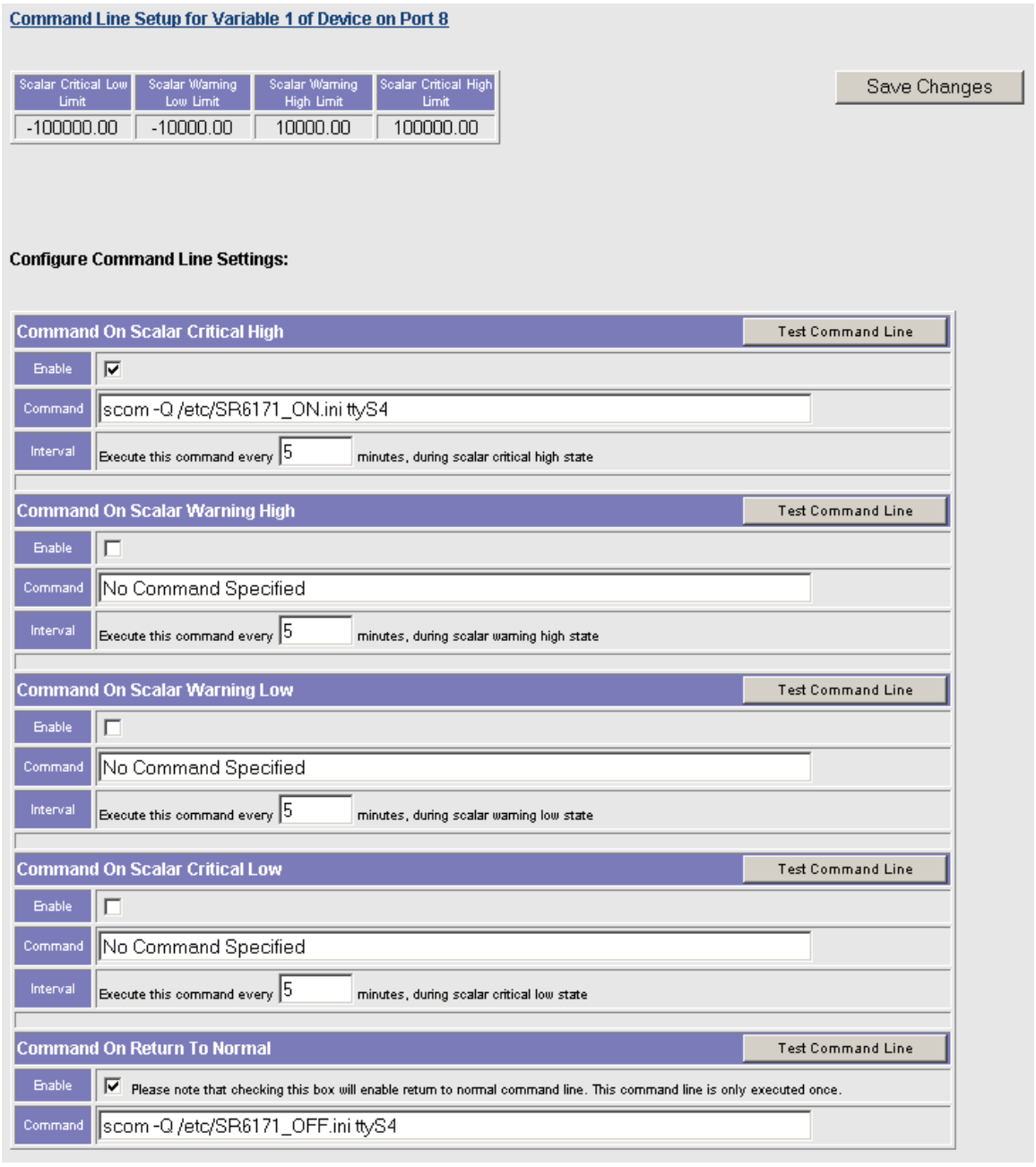


Figure 17: Configuring Command Line Alerts for a Scalar Variable

In the example shown in Figure 17, above, the Alert appliance will turn ON a relay connected to port 4 when the reading exceeds the Scalar Critical High Limit, and will turn OFF the relay when the reading returns to normal.

4. In order to turn a relay on, you will need to enter the following command in the **Command** field:

   scom -Q /bin/SR6171_ON.ini ttyS4

   In order to turn a relay off, you will need to enter the following in the **Command** field:

   scom -Q /bin/SR6171_OFF.ini ttyS4

In the command lines above, ttyS4 is the name used to access serial port 4. The relay can be connected to any serial port on the back of the Alert appliance. As an example, if the relay was connected on serial port 8, use ttyS8 in the command line.

5. For each command line alert that you would like to enable, check the corresponding **Enable** checkbox.
6. Click on the **Save Changes** button.
7. It is highly recommended that you test all of your commands to ensure that they are properly setup. You can test each command by clicking on its **Test Command Line** button.

Upgrading the firmware on your Alert Appliance

Sensorsoft recommends that you keep your Alert appliance's firmware up-to-date. This way you can take advantage of the latest enhancements and bug fixes. To check for new a firmware release, go to the following URL:

http://www.sensorsoft.com/ssalert_images.html

Accessing Sensorsoft devices on Alert with other monitoring software

The Sensorsoft devices that are attached to your Alert appliance can be accessed and monitored by other Sensorsoft monitoring products. This is possible because your Alert appliance has device server capability to share its serial ports on the network. Each serial port on your Alert appliance can be accessed through the IP address of the appliance plus the TCP port number corresponding to the serial port. For each serial port, its corresponding TCP port number is determined by adding 3000 to its serial port number. For example, serial port 2 of your Alert appliance is shared on TCP port 3002, and serial port 4 of your Alert appliance is shared on TCP port 3004.

To allow other monitoring products to access a particular Sensorsoft device on your Alert appliance, you must enable the device for monitoring (Refer to section *Monitoring a Sensorsoft Device*). Please note that your Alert appliance can share only Sensorsoft devices with Sensorsoft monitoring software, and not third party plug-in supported devices.

The following is a list of products that can monitor Sensorsoft devices on Alert:

- Sensorsoft Remote Watchman Enterprise (RWME)
- Sensorsoft Remote Watchman Client (RWMC)
- Sensorsoft SCOM Serial Communications Tool

To use the above products to monitor Sensorsoft devices through TCP ports, please refer to their respective user manual.

Managing multiple Alert Appliances with RWME Software

Sensorsoft Remote Watchman Enterprise (RWME) software (Build 94a and forward) can centralize the management of multiple Alert appliances. RWME software is sold separately. Using RWME, you can conveniently see the status of all the Alert appliances in your organization from a list based view. The status will tell you whether each appliance is online, whether any alert conditions or exceptions has occurred on each appliance, and whether web login passwords on each appliance have changed. RWME can also log you into each Alert appliance's web interface with just one mouse click. All these features allow you to manage multiple Alert appliances without having to manually login to each one.

If you have RWME Build 94a or greater, and would like to learn how to manage Alert appliances using RWME, please refer to the RWME user manual.

Root User

The **root** username is used to login to Alert's Linux shell. The default root password is **sensorsoft**. It is recommended that you change the root password on the Sensorsoft Alert appliance as soon as possible. The following procedure outlines how to do this.

Changing the root password

1. Connect to the Sensorsoft Alert appliance through Secure Shell or through the serial console. If the Alert appliance has not been configured with valid IP settings, then you must connect to it through the serial console (See the section *Connecting to the Alert Serial Console*).
2. Login as: **root**
3. At the prompt, type **passwd** and then press **Enter**
4. Enter your new root password and then confirm it by entering it one more time.
5. At the command prompt, type **saveconf** and then press **Enter**
6. Your new root password is now activated. You will need this password to login to the Alert appliance through Secure Shell or the serial console.

Recovering from a lost root password

Model SSA7001

If you have changed the root password of your Alert appliance from the default: **sensorsoft**, you will need to recover by using the following procedure:

1. If the Alert appliance is currently running, then shut it down using the web interface (Refer to section *Appliance Shutdown and Reboot* for how to do this). If you have lost the Alert appliance's web password then simply skip this step.
2. Connect to the Sensorsoft Alert appliance though the serial console (Refer to section *Connecting to the Alert Serial Console*).
3. At the command prompt, type **passwd** and then press E**nter**.
4. Enter your new root password and then confirm it by entering it one more time.
5. At the command prompt, type **saveconf** and then press E**nter**.
6. At the command prompt, type **reboot** and then press **Enter**. The appliance will now reboot.
7. After the Alert appliance reboots, your new root password will be activated. You will need this password to login to the Alert appliance through Secure Shell.

Models SSA7004 and SSA7008

If you have changed the root password of your Alert appliance from the default: **sensorsoft**, you will need to recover by following the procedure below. To begin, you need the following items:

- A host computer with a spare serial port.
- The P/N C4003 adaptor or the P/N C4005 adaptor. Both of these adaptors came with your Alert appliance, and are gray colored. The P/N C4003 adaptor has a DB-9F connector. The P/N C4004 adaptor has DB-25F connector. Choose the one that fits the spare serial port of your host computer.

- The P/N C2013 cable that came with your Alert appliance. This is a blue RJ-45 straight-through cable.

1. If the Alert appliance is currently running, then shut it down using the web interface (Refer to section *Appliance Shutdown and Reboot* for how to do this). If you have lost the Alert appliance's web password then simply skip this step.
2. Power off the Alert appliance using the ON/OFF switch located on the back of the Alert Appliance.
3. Connect one end of the blue RJ-45 straight-through cable to the serial console port on the Alert appliance. The serial console port is located on the back of the appliance, and is labeled "CONSOLE".
4. Connect the other end of the blue RJ-45 straight-through cable to the gray colored connector labeled "Console".
5. Connect the gray connector to the serial port on your host computer.
6. Launch a terminal emulation program on your host computer. If your host computer's operating system is Windows 95, 98, Me, NT, 2K, or XP, you can use HyperTerminal located under Start > Program > Accessories. If your host computer's operating system is UNIX, you can use either Kermit or Minicom.
7. Configure the terminal parameters as shown below, and then connect.
   - Serial Speed: 9600 bps
   - Data Bits: 8 bits
   - Parity: None
   - Stop Bits: 1
   - Flow Control: None
   - Emulation: ANSI
8. Power up the Alert appliance using the ON/OFF switch located on the back of the appliance.
9. As the appliance is booting up it will output the following on the terminal:

   Entry Point = 0x00002120
   loaded at: 00002120 0000D370
   relocated to: 00300020 0030B270
   board data at: 003052C8 0030537C
   relocated to: 002FF120 002FF1D4
   zimage at: 00008100 0006827E
   relocated to: 00DB7000 00E1717E
   initrd at: 0006827E 0024F814
   relocated to: 00E18000 00FFF596
   avail ram: 0030B270 00E18000
   Linux/PPC load: root=/dev/ram

10. After "**Linux/PPC load: root=/dev/ram**" is printed, you have 4 seconds to enter the following: "**<SP>single<Enter>**" (One press of the **space** bar and then the word "**single**" and then press the **Enter** key**)**.
11. This will allow you to access the Sensorsoft Alert Appliance in single user mode.
12. You will see the following prompt: **[root@(none) /]#**
13. At the prompt type **passwd** and press the **Enter** key
14. Enter a new root password and then reenter it to confirm.
15. At the prompt type **saveconf** and press the **Enter** key
16. At the prompt type **reboot** and press the **Enter** key. The Alert appliance will now reboot.
17. After the appliance has rebooted, the new root password will be active.

Backup files on Alert appliance to a remote host

There are several circumstances where you may want to backup files on your Alert appliance to a remote host. We provide example methods below for doing this using scp and tftp. The scp (secure copy) command lines assume you have a Unix or Linux host that has a ssh/sftp server installed and running. The tftp (trivial ftp) command lines assume you have a Windows or Unix/Linux host that has a tftp[1] server installed and running. After executing the scp commands it will prompt you for the password of the remote user. The command lines shown are executed from your Alert appliance root login.

Backup flash settings (script) file to a remote host

If your script file becomes corrupt it will mean all of your user settings are lost. Therefore taking the time to back up the script file will allow for a speedy recover instead of the lengthy process of having to renter all your settings.

After you have saved your Alert appliance settings using the saveconf command you can backup for safe keeping the script file. The commands below can be used to periodically backup the script file.

CAUTION – Do not run the following commands if you are having problems accessing the web interface of the Alert appliance. Otherwise you could create a corrupt script backup file or overwrite a known good script backup file.

```
# saveconf
# scp /proc/flash/script username@remotehost:/home/username/alertbackup/script.backup
```

or

```
# saveconf
# tftp -l /proc/flash/script  -r script.backup  -p tftp_server
```

Backup log files to a remote host

Since the Alert log files are lost at every reboot you can periodically save these files to a remote host should you require this information for archival purposes.

```
# scp /logs/*.log  username@unixhost:/home/username/alertbackup/
```

The tftp method below requires each log file to be transferred separately. You can automate this by including them in a Linux shell script:

```
# tftp -l /logs/_Port01_Var1.log  -r _Port01_Var1.log -p tftp_server
```

[1] A free open-source TFTP server for Windows is available for download at http://tftpd32.jounin.net/

Restore known good script backup file to Alert appliance from a remote host

If you are experiencing problems accessing the Alert web interface you may have a corrupt script file. Try starting the alertd process from the command line as follows:

```
# /bin/alertd
```

If you get the error message “unsupported platform” you have a corrupt script file. The following commands will allow you to restore a known good script backup file to your Alert appliance from a remote host:

```
# scp username@remotehost:/home/username/alertbackup/script.backup \
/proc/flash/script
# reboot
```

or

```
# tftp -l /proc/flash/script  -r script.backup -g tftp_server
# reboot
```

After the Alert appliance is allowed time to reboot you should be able to access its web interface.

SNMP Interface

Sensorsoft Alert SNMP Agent Specifications

SNMP Version supported	1
Commappliancey Names	Multiple commappliancеies with read and write permissions
Max number of Boolean or Scalar class variables supported per SSD	8
Device Access Method	Indexed
Variable Access Method	Indexed
Number of Sensorsoft MIB Objects	73
Starting MIB OID	.1.3.6.1.4.1.15848.1.1.0

Scalar and Boolean class Variables

Device variables can be classified in terms of the way they represent their data. Scalar variables are those values that are represented by a range of possible numbers. Devices that monitor temperature or humidity are classified as scalar. Boolean variables define only two states: binary one or zero. Devices that monitor power (PWR FAIL/PWR OK), flooding (WET/DRY), or control a relay position (ON/OFF) are classified as Boolean.

The distinction between scalar and Boolean is important because it influences the way data is retrieved from the Sensorsoft SNMP Agent. If you examine the MIB, you will notice objects prefixed with *Scalar* or *Boolean*. Only one set of variables is of interest to you, depending on the type of SSD being used. When using a Scalar SSD the values of the MIB objects prefixed with or containing Scalar are used and those prefixed with or containing Boolean are not used. When using a Boolean SSD, the values of the MIB objects prefixed with or containing Boolean are used and those prefixed with or containing Scalar are not used. Refer to section *Description of Alert MIB Objects* section for a more detailed description of each MIB object.

Sensorsoft Alert MIB

The typical way to manipulate the Sensorsoft Alert SNMP Agent's variables is to load the provided MIB into a third party, Network Management Software (NMS) that can act as an interface between the user and the Sensorsoft Alert SNMP Agent.

The Sensorsoft Alert MIB file can be downloaded from:

http://www.sensorsoft.com/download/alertmib1.mib

You should load the MIB into your NMS as per the procedure recommended by the manufacturer. You may refer to section *Description of Alert MIB Objects* for a complete list of objects in the Sensorsoft Alert MIB.

Sensorsoft Alert Indexed MIB Usage

Readings from device variables are accessed through the **ssVarReading** MIB object. Although your Alert appliance could be monitoring multiple devices, and each device could contain multiple variables, the Sensorsoft SNMP Agent allows access to one variable on one device at a time. The variable that is currently being accessed is controlled by the variable index stored in **ssVarIndex**, and the device index stored in **ssDeviceIndex**. Setting **ssVarIndex** or **ssDeviceIndex** to a new value changes the variable that is being accessed, so that all subsequent GET and SET operations operate on that variable. For example, to get the reading of variable 2 on the device connected to port 4, do the following:

1. Set **ssDeviceIndex** to 4
2. Set **ssVarIndex** to 2
3. Get **ssVarReading**

ssVarReading is an example of a MIB object that is indexed by both **ssDeviceIndex** and **ssVarIndex**. Other such objects are **ssApplianceOfMeasure, ssScalarCriticaHighLimit** and **ssEmailOnScalarCriticalHighEnable**.

Some Alert MIB objects are indexed by **ssDeviceIndex** only, such as **ssDeviceLocation**, and **ssDeviceModel**. The value of **ssVarIndex** has no effect on these objects.

Setting Breach Limits on Scalar Variables

The reading of the currently indexed scalar variable on the currently indexed device is given by the **ssScalarData** MIB object. The appliance of measure of this scalar data is given by the **ssApplianceOfMeasure** MIB object. You may also obtain both the reading and the appliance of measure together in the **ssVarReading** MIB object.

Breach limits can be defined for each scalar variable so that when the variable's reading exceeds a particular breach limit, the variable will enter an alert state. Four different breach limits can be set through the following MIB objects:

- ssScalarCriticalLowLimit
- ssScalarWarningLowLimit
- ssScalarWarningHighLimit
- ssScalarCriticalHighLimit

These breach limits in turn define the conditions in which a scalar variable will enter the following alert states.

- Breach Of Critical Low Limit
- Breach of Warning Low Limit
- Return To Normal
- Breach of Warning High Limit
- Breach of Critical High Limit

Different alert actions can be taken in each alert state. The following alert actions are supported:

- Email
- SMS-Paging (SSA7004 and SSA7008 only)
- SNMP Traps
- Command line execution

Any combination of these alert actions can be taken when a scalar variable enters a particular alert state. Please note that SMS-Paging cannot be configured through SNMP. Please use the Alert web interface to configure any SMS-Paging alerts.

To enable a specific alert action for a particular alert state, the corresponding **ss***XXXXXX***Enable** MIB object must be set to 1. The following chart lists the **ss***XXXXXX***Enable** objects that correspond to each alert action for each alert state:

Alert State	Trap Enable Object	Email Enable Object	Command Line Enable Object
Breach of Critical High Limit	**SsTrapOnScalarCriticalEnable**	**SsEmailOnScalarCriticalEnable**	**ssCommandOnScalarCriticalHighEnable**
Breach of Warning High Limit	**SsTrapOnScalarWarningEnable**	**SsEmailOnScalarWarningEnable**	**ssCommandOnScalarWarningHighEnable**
Return To Normal	**SsTrapOnReturnToNormalEnable**	**SsEmailOnReturnToNormalEnable**	**SsCommandOnReturnToNormalEnable**
Breach of Warning Low Limit	**SsTrapOnScalarWarningEnable**	**SsEmailOnScalarWarningEnable**	**ssCommandOnScalarWarningLowEnable**
Breach of Critical Low Limit	**SsTrapOnScalarCriticalEnable**	**SsEmailOnScalarCriticalEnable**	**ssCommandOnScalarCriticalLowEnable**

For instance, to have a trap and an Email sent whenever the currently indexed variable on the currently indexed device enters the Breach of Warning High Limit state, you should set **ssTrapOnScalarWarningEnable** and **ssEmailOnScalarWarningEnable** to 1.

Setting Breach Limit on Boolean Variables

The reading of the currently indexed Boolean variable on the currently indexed device is given by the **ssBooleanData** MIB object.

A Boolean variable will enter alert state when its reading is equal to the user defined Boolean critical value. The Boolean critical value is set through the **ssBooleanCriticalState** MIB object, and can be assigned one of the two possible Boolean values. The two possible Boolean values are stored in the MIB objects **ssBooleanZeroStateString** and **ssBooleanOneStateString**. For example, to be alerted when your power sensor detects power failure, set **ssBooleanCriticalState** to "*PWR FAIL*".

There are two possible alert states for each Boolean variable:

- Breach Of Boolean Critical Limit
- Return to Normal

Different alert actions can be taken in each alert state. The following alert actions are supported:

- Email
- SMS-Paging (SSA7004 and SSA7008 only)
- SNMP Traps
- Command line execution

Any combination of these alert actions can be taken when the variable enters a particular alert state. Please note that SMS-Paging cannot be configured through SNMP. Please use the Alert web interface to configure any SMS-Paging alerts.

To enable a specific alert action for a particular alert state, the corresponding **ss***XXXXXX***Enable** MIB object must be set to 1. The following chart lists the **ss***XXXXXX***Enable** objects that correspond to each alert action for each alert state:

Alert State	Trap Enable MIB Object	Email Enable MIB Object	Command Line Enable MIB Object
Breach of Boolean Critical Limit	**SsTrapOnBooleanCriticalEnable**	**SsEmailOnBooleanCriticalEnable**	**ssCommandOnBooleanCriticalEnable**
Return To Normal	**SsTrapOnReturnToNormalEnable**	**SsEmailOnReturnToNormalEnable**	**SsCommandOnReturnToNormalEnable**

For instance, to have a trap and an Email sent whenever the currently indexed variable on the currently indexed device enters the Breach of Boolean Critical Limit state, you should set **ssTrapOnBooleanCriticalEnable** and **ssEmailOnBooleanCriticalEnable** to 1.

Setting up SNMP Trap Alerts

1. **Setting the Trap Destination IP Address:**
   Set the **ssTrapDestination1** object to the IP address of the network management station where you would like to receive traps. If you would like to receive SNMP traps at two different network management stations, set the **ssTrapDestination2** object to the IP address of the second station.
2. **Selecting the monitored device for which alerts will be setup:**
   This is done by setting the **ssDeviceIndex** MIB object to the index of the serial port where the monitored device is connected. For instance, if you would like to send a trap when a temperature is too high, and you have a SS6610J sensor connected to port 2, set **ssDeviceIndex** to 2.
3. **Selecting the variable for which alerts will be setup:**
   This can be done by setting the **ssVarIndex** object. For instance, the SS6610J Sensor has 4 variables. The first two variables (**ssVarIndex** =1 and **ssVarIndex**=2) are humidity variables. The next two variables on the SS6610J Sensor are temperature variables (**ssVarIndex** =3 and **ssVarIndex**=4). You can easily tell which variable you are currently accessing by doing an SNMP Get on the **ssVarName** object.
4. **Setting breach limits on the variable:**
   There are two different classes of variables on Sensorsoft devices and Sensorsoft plug-in supported devices. They are scalar and Boolean. You can determine the class of the currently indexed variable on the currently indexed device by getting **ssVarClass** object's value. **If the variable is scalar, proceed with step 5. If the variable is Boolean, skip step 5 and continue with step 6.**
5. **Setting scalar breach limits if the variable is scalar:**
   Refer to section *Setting Breach Limits on Scalar Variables through SNMP* for how to setup the scalar breach limits. If you want to be alerted by a trap when this variable goes into Breach of Scalar Critical state, set **ssTrapOnScalarCriticalEnable** to 1; if you want be alerted by a trap when this variable goes into Breach Of Scalar Warning state, set **ssTrapOnScalarWarningEnable** to 1. To disable a trap, set the **ssTrapOnScalarCriticalEnable** or **ssTrapOnScalarWarningEnable** object back 0. By default, traps will be repeatedly sent at 5 minute intervals as long as the variable is in the same breach state. You can change this alerting interval by specifying a new value (in minutes) in **ssTrapOnScalarCriticalInterval** and **ssTrapOnScalarWarningInterval**.
6. **Choosing the Boolean critical value if the variable is Boolean:**
   Please refer to section *Setting Breach Limit on Boolean Variables through SNMP* for how to set the **Boolean critical value**. Once we have set the **ssBooleanCriticalState** Object, we must enable the trap

by setting the **ssTrapOnBooleanCriticalEnable** to 1. By default, traps will be repeatedly sent at 5 minute intervals as long as the variable is in breach state. You can change this alerting interval by specifying a new value (in minutes) in **ssTrapOnBooleanCriticalInterval**.

7. **Setting up the return to normal traps:**
   Now that you have setup the traps to be sent in the breach conditions, you may also want a trap sent when the variable's reading returns back to normal. For instance, to have a trap sent when the currently indexed variable returns to a normal state, you should set the **ssTrapOnReturnToNormalEnable** object to 1.

Structure of SNMP Traps from Sensorsoft Alert

When the Alert appliance starts up, it will send a **coldStart** trap. When it shuts down, it will send a **linkDown** trap. During operation of the Alert appliance, there are 1 to 8 enterprise specific traps that may be sent out. The actual number of unique enterprise specific traps depends on the number of ports on your Alert appliance. For instance, an 8 port appliance will have 8 enterprise specific traps, whereas a 4 port appliance will only have 4. The specific trap number corresponds with the serial port which the monitored device is connected to. For instance, if your NMS receives an enterprise specific trap from the Alert appliance, and the trap number is 4, then the trap must have originated from an event on the device connected to serial port 4. To find out what alert condition caused the trap, you must look at the trap's variable bindings.

Variable Bindings of Sensorsoft Alert Traps

Every enterprise specific trap of Sensorsoft Alert has the variable bindings listed below. You can refer to section *Description of Alert MIB Objects* for more information about each variable.

ssApplianceLocation
The physical location of the appliance

ssDeviceLocation
The physical location of the monitored device that generated this particular trap

ssDeviceIndex
The index of the serial port to which the monitored device is connected

ssDeviceStatus
The status of the monitored device

ssVarIndex
The index of the variable that caused this particular trap to be issued

ssVarStatus
The status of the variable that caused this particular trap to be issued

Setting up Email Alerts through SNMP

1. **Setting the Primary and Secondary SMTP Server Addresses:**
   In order to send out email alerts from the Alert appliance, you must set the **ssPrimarySMTPServer** MIB object to the address of your SMTP server. If you would like to specify a backup SMTP server to use in case the primary SMTP server fails, set the **ssSecondarySMTPServer** MIB object to the address of your backup SMTP server.
2. **Selecting the monitored device for which alerts will be setup:**

This is done by setting the **ssDeviceIndex** MIB object to the index of the serial port where the monitored device is connected. For instance, if you would like to send a trap when a temperature is too high, and you have a SS6610J sensor connected to port 2, set **ssDeviceIndex** to 2.

3. **Selecting the variable for which alerts will be setup:**
   This is done by setting the **ssVarIndex** MIB object to the index of the variable to be alerted on. For instance, the SS6610J sensor has 4 variables. The first two variables (**ssVarIndex**=1 and **ssVarIndex**=2) are humidity variables. The next two variables on the SS6610J sensor are temperature variables (**ssVarIndex**=3 and **ssVarIndex**=4). You can find out which variable you are currently accessing to by doing an SNMP Get on the **ssVarName** MIB object.

4. **Setting breach limits on the variable:**
   There are two different classes of variables on Sensorsoft devices and Sensorsoft plug-in supported devices. They are scalar and Boolean. You can determine the class of the currently indexed variable on the currently indexed device by doing an SNMP Get on the **ssVarClass** MIB object. **If the variable is scalar, proceed with step 5. If the variable is Boolean, skip step 5 and continue with step 6.**

5. **Setting scalar breach limits if the variable is scalar:**
   Please refer to section *Setting Breach Limits on Scalar Variables through SNMP* for how to setup scalar breach limits. To be alerted when this variable goes into Breach of Scalar Critical state, set the **ssEmailOnScalarCriticalEnable** MIB object to 1. To be alerted when this variable goes into Breach of Scalar Warning state, set the **ssEmailOnScalarWarningEnable** MIB object to 1. By default, emails will be repeatedly sent at 5 minute intervals as long as the variable is in the same breach state. You can change this alerting interval by specifying a new value (in minutes) in **ssEmailOnScalarCriticalInterval** and **ssEmailOnScalarWarningInterval**. For instance, to receive an email alert every five minutes when the variable is in the Breach of Scalar Critical state, you would first set the **ssEmailOnScalarCriticalEnable** to 1 and then you would set the **ssEmailOnScalarCritical** interval to 5. You can also customize the email that is sent by modifying the **ssEmailOnScalarCriticalSubject**, **ssEmailOnScalarCriticalMessage** and the **ssEmailOnScalarCriticalAddresses** MIB objects. Please note that when setting the **ssEmailOnScalarCriticalAddresses** object, multiple email addresses must be delimited by commas. **Please continue with step 7**.

6. **Choosing Boolean critical value if the variable is Boolean:**
   Please refer to section *Setting Breach Limit on Boolean Variables through SNMP* for how to set the Boolean critical value. Once we have set the **ssBooleanCriticalState** Object, we must enable the email by setting the **ssEmailOnBooleanCriticalEnable** to 1. By default, emails will be repeatedly sent at 5 minute intervals as long as the variable is in breach state. You can change this alerting interval by specifying a new value (in minutes) in **ssEmailOnBooleanCriticalInterval**.

7. **Setting up the return to normal emails:**
   Now that we have setup the emails to be sent in the case of a breach condition, you may also want an email sent when the variable's reading returns back to normal. For instance, to be alerted by email when the currently indexed variable returns to a normal state, you should set the **ssEmailOnReturnToNormalEnable** object to 1.

Setting up Command Line Alerts through SNMP

Command line alerts can turn relays on or off in response to alert conditions. For instance, if a particular temperature variable goes above a certain limit, the Alert appliance could turn on an SR6171J Sensorsoft relay in response. The relay could in turn sound an alarm. The following are steps to setup command line alerts through SNMP.

1. **Selecting the monitored device for which alerts will be setup:**

This is done by setting the **ssDeviceIndex** MIB object to the index of the serial port where the device is connected. For instance, if you would like to execute a command line when a temperature is too high, and you have a SS6610J sensor connected to port 2, set **ssDeviceIndex** to 2.

2. **Selecting the variable for which alerts will be setup:**
   This is done by setting the **ssVarIndex** MIB object to the index of the variable to be alerted on. For instance, the SS6610J Sensor has 4 variables. The first two variables (**ssVarIndex**=1 and **ssVarIndex**=2) are humidity variables. The next two variables on the SS6610J Sensor are temperature variables (**ssVarIndex**=3 and **ssVarIndex**=4). You can easily tell which variable you are currently accessing by doing an SNMP Get on the **ssVarName** MIB object.
3. **Setting breach limits on the variable:**
   There are two different classes of variables on Sensorsoft devices and Sensorsoft Plug-in supported devices. They are scalar and Boolean. You can determine the class of the currently indexed variable by doing an SNMP Get on **ssVarClass**. **If the variable is scalar, proceed with step 5. If the variable is Boolean, skip step 5 and continue with step 6.**
4. **Setting up the scalar breach limits if the variable is scalar:**
   Please refer to section *Setting Breach Limits on Scalar Variables through SNMP* for how to setup scalar breach limits. Enable the command lines for the scalar breach states that you would like to be alerted on by setting the corresponding Enable MIB objects (**ssCommandOnScalarCriticalLowEnable**, **ssCommandOnScalarWarningLowEnable**, **ssCommandOnScalarWarningHighEnable** and **ssCommandOnScalarCriticalHighEnable**) to 1. For each command line alert that is enabled, you need to specify the command line to be executed. The MIB objects, **ssCommandOnScalarCriticalLow**, **ssCommandOnScalarWarningLow**, **ssCommandOnScalarWarningHigh** and **ssCommandOnScalarCriticalHigh** should be set with the appropriate command lines. For a description of the command lines used to turn an SR6171J relay on or off, refer to *Appendix B*. By default, command lines will be repeatedly executed at 5 minute intervals as long as the variable is in breach state. You can change this alerting interval by specifying a new value (in minutes) in **ssCommandOnScalarCriticalLowInterval**, **ssCommandOnScalarWarningLowInterval**, **ssCommandOnScalarWarningHighInterval** and **ssCommandOnScalarCriticalHighInterval**. **Please continue with step 6**.
5. **Choosing the Boolean critical value if the variable is Boolean:**
   Please refer to section *Setting Breach Limit on Boolean Variables through SNMP* for how to set the Boolean critical value. Once you have set the **ssBooleanCriticalState** Object, you must enable the command line alert by setting **ssCommandOnBooleanCriticalEnable** to 1. Then you should specify the command line to execute in the **ssCommandOnBooleanCritical** MIB object. For a description of command lines to control the Sensorsoft SR6171J Relay, please refer to *Appendix B*. By default, command lines will be repeatedly executed at 5 minute intervals as long as the variable is in breach state. You can change this alerting interval by specifying a new value (in minutes) in **ssCommandOnBooleanCriticalInterval**.
6. **Setting up the return to normal command line alerts:**
   Now that you have setup the command lines to be executed in the case of breach conditions, you may want a command line executed when the variable's reading returns back to normal. For instance, to turn a relay off when the currently indexed variable returns to a normal value, set the **ssCommandOnReturnToNormalEnable** MIB object to 1. For a description of command lines to control the Sensorsoft SR6171J Relay, please see *Appendix B*.

Description of Alert MIB Objects

This section lists and describes all of the objects contained in the Sensorsoft MIB. In addition to the name and description, the following information is given:

Type	The object type describes the variable type of the object. Typical variable types include *IPAddress, Integer,* and *String.* Attempting to enter an invalid value (for example, the string "hello" for a variable that requires a number) will usually result in an error message being returned to the NMS. When changing a value, always verify that the change actually occurred, by doing an SNMP Get.
Access	Specifies the read and write access granted for the object. It can be *Read/Write* or *Read only*. Variables that are *Read only* indicate that the variable is provided for informational purposes and cannot be set by the user.
OID	The specific Object Identifier for the object. This may be required by some SNMP tools to specifically reference the variable. Most NMS software will allow you to refer to the variable name, and will keep track of the OID for you.
Non-Volatile	Objects marked non-volatile are saved between sessions. That is, if the Sensorsoft Alert appliance loses power (either deliberately or accidentally), the Agent's non-volatile objects will not lose their values.

Note that many network management software packages can extract this information directly from the MIB. Consult your NMS software's documentation for information on how to view the following information from your NMS.

ssApplianceLocation

DESCRIPTION: The physical location of the Sensorsoft Alert appliance.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.1.0

Non-volatile

ssApplianceModelNumber

DESCRIPTION: The model number of the Sensorsoft Alert appliance.

TYPE: String

ACCESS: Read Only

OID .1.3.6.1.4.1.15848.1.2.0

ssSoftwareVersion

DESCRIPTION: The version number of the software on the Sensorsoft Alert appliance.

TYPE: String

ACCESS: Read Only

OID .1.3.6.1.4.1.15848.1.3.0

ssNumberOfPorts

DESCRIPTION: The number of serial ports on the Sensorsoft Alert appliance.

TYPE: Integer

ACCESS: Read Only

OID .1.3.6.1.4.1.15848.1.4.0

ssTrapDestination1

DESCRIPTION: The destination IP address for sending traps to the first NMS.

TYPE: IP address, of the form xxx.xxx.xxx.xxx

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.5.0

Non-volatile

ssTrapDestination2

DESCRIPTION: The destination IP address for sending traps to the second NMS.

TYPE: IP address, of the form xxx.xxx.xxx.xxx

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.6.0

Non-volatile

ssPrimarySMTPServer

DESCRIPTION: This is the address of the primary SMTP server that will be used to send email alerts.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.7.0

Non-volatile

ssSecondarySMTPServer

DESCRIPTION: This is the address of the secondary SMTP server that will only be used to send email alerts if the primary SMTP server fails.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.8.0

Non-volatile

ssEmailAlertSenderAddress

DESCRIPTION: This is the email address of the sender when an email alert is issued. All email alerts will be from this address.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.9.0

Non-volatile

ssDeviceIndex

DESCRIPTION: The user-defined index to select a particular device. The device on the first port is 1, the device on the second port is 2 and so on. This index will affect the contents of all objects below.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.10.0

ssDeviceModel

DESCRIPTION: The model number of the currently indexed device.

TYPE: String

ACCESS: Read Only

OID .1.3.6.1.4.1.15848.1.11.0

ssDeviceLocation

DESCRIPTION: The user-definable text describing the physical location of the currently indexed device.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.12.0

Non-volatile

ssDeviceDescription

DESCRIPTION: The user-definable description of the currently indexed device.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.13.0

Non-volatile

ssDeviceStatus

DESCRIPTION: The status of the currently indexed device. The status can be Normal, TIMEOUT - Device not responding, OFFLINE - TCP connection problem, LOW VOLTAGE, EEPROM FAILURE or TAMPER DETECTED.

TYPE: String

ACCESS: Read Only

OID .1.3.6.1.4.1.15848.1.14.0

ssNumVariables

DESCRIPTION: The total number of variables supported by the currently indexed device.

TYPE: Integer

ACCESS: Read Only

OID .1.3.6.1.4.1.15848.1.15.0

ssVarIndex

DESCRIPTION: The user-defined index to select a particular variable in the currently indexed device. This index should not be less than 1 or greater than ssNumVariables above. This index will affect the contents of all objects below.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.16.0

ssVarName

DESCRIPTION: The name of the currently indexed variable on the currently indexed device.

TYPE: String

ACCESS: Read Only

OID .1.3.6.1.4.1.15848.1.17.0

ssVarClass

DESCRIPTION: The class (either Boolean or scalar) of the currently indexed variable on the currently indexed device.

TYPE: String

ACCESS: Read Only

OID .1.3.6.1.4.1.15848.1.18.0

ssVarReadWriteCapability

DESCRIPTION: This indicates whether the currently indexed variable can be read or written (i.e. RO means read only, RW means read and write).

TYPE: String

ACCESS: Read Only

OID .1.3.6.1.4.1.15848.1.19.0

ssVarReading

DESCRIPTION: The currently indexed variable's reading. The reading is either ssBooleanData or ssScalarData along with the ssApplianceOfMeasure, depending on the ssVarClass of the currently indexed variable on the currently indexed device

TYPE: String

ACCESS: Read Only

OID .1.3.6.1.4.1.15848.1.20.0

ssVarStatus

DESCRIPTION: The status of the currently indexed variable. The status can be: Normal, Breach of Boolean Critical Limit, Breach of Critical High Limit, Breach of Critical Low Limit, Breach of Warning Low Limit, Breach of Warning High Limit and Returned to Normal status.

TYPE: String

ACCESS: Read Only

OID .1.3.6.1.4.1.15848.1.21.0

ssScalarData

DESCRIPTION: The device's data, if the currently indexed variable on the currently indexed device is of the scalar class.

TYPE: Integer

ACCESS: Read-Write

OID .1.3.6.1.4.1.15848.1.22.0

ssApplianceOfMeasure

DESCRIPTION: The appliance of measure for the scalar data. For example, if the currently indexed variable is a temperature reading, then the appliance of measure will be either F for Fahrenheit or C for Celsius. Boolean variables do not have appliance of measure.

TYPE: String

ACCESS: Read Only

OID .1.3.6.1.4.1.15848.1.23.0

ssScalarCriticalHighLimit

DESCRIPTION: If the currently indexed variable is of scalar class, then this represents the limit that the scalar data must reach, or rise above, before this variable enters Breach of Critical High Limit status.

TYPE: Integer

ACCESS: Read-Write

OID .1.3.6.1.4.1.15848.1.24.0

Non-volatile

ssScalarWarningHighLimit

DESCRIPTION: If the currently indexed variable is of scalar class, then this represents the limit that the scalar data must reach, or rise above, before this variable enters Breach of Warning High status.

TYPE: Integer

ACCESS: Read-Write

OID .1.3.6.1.4.1.15848.1.25.0

Non-volatile

ssScalarWarningLowLimit

DESCRIPTION: If the currently indexed variable is of scalar class, then this represents the limit that the scalar data must reach, or fall below, before this variable enters Breach of Warning Low status.

TYPE: Integer

ACCESS: Read-Write

OID .1.3.6.1.4.1.15848.1.26.0

Non-volatile

ssScalarCriticalLowLimit

DESCRIPTION: If the currently indexed variable is of scalar class, then this represents the limit that the scalar data must reach, or fall below, before this variable enters Breach of Critical Low status.

TYPE: Integer

ACCESS: Read-Write

OID .1.3.6.1.4.1.15848.1.27.0

Non-volatile

ssBooleanData

DESCRIPTION: The device's data, in the form of a state string, if the currently indexed variable on the currently indexed device is of the Boolean class. The string will correspond to either the ssBooleanOneStateString or ssBooleanZeroStateString objects.

TYPE: String

ACCESS: Read-Write

OID .1.3.6.1.4.1.15848.1.28.0

ssBooleanOneStateString

DESCRIPTION: The device's one-state string, if the currently indexed variable is of the Boolean class. (i.e ON, CLOSED, WET or PWR_FAIL).

TYPE: String

ACCESS: Read only

OID .1.3.6.1.4.1.15848.1.29.0

ssBooleanZeroStateString

DESCRIPTION: The device's zero-state string, if the currently indexed variable is of the Boolean class. (i.e OFF, OPEN, DRY or PWR_OK).

TYPE: String

ACCESS: Read only

OID .1.3.6.1.4.1.15848.1.30.0

ssBooleanCriticalState

DESCRIPTION: The user-definable state string, if the currently indexed variable is of the Boolean class. (This string must be the value of either ssBooleanOneStateString or ssBooleanZeroStateString, depending on which state you would like to be alerted on).

TYPE: String

ACCESS: Read only

OID .1.3.6.1.4.1.15848.1.31.0

ssTrapOnScalarCriticalEnable

DESCRIPTION: A zero value disables this trap. A value of one enables this trap. When enabled, this trap is sent when the agent detects that the currently indexed variable on the currently indexed device enters a Breach of Critical High Limit status or Breach of Critical Low Limit status. It will be sent periodically using the time interval in minutes specified by ssTrapOnScalarCriticalInterval.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.32.0

Non-volatile

ssTrapOnScalarCriticalInterval

DESCRIPTION: The time interval in minutes between traps when the agent detects that the currently indexed variable on the currently indexed device enters a Breach of Critical High Limit status or Breach of Critical Low Limit status.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.33.0

Non-volatile

ssTrapOnScalarWarningEnable

DESCRIPTION: A zero value disables this trap. A value of one enables this trap. When enabled, this trap is sent when the agent detects that the currently indexed variable on the currently indexed device enters a Breach of Warning High Limit status or Breach of Warning Low Limit status. It will be sent periodically using the time interval in minutes specified by ssTrapOnScalarWarningInterval.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.34.0

Non-volatile

ssTrapOnScalarWarningInterval

DESCRIPTION: The time interval in minutes between traps when the agent detects that the currently indexed variable on the currently indexed device enters a Breach of Warning High Limit status or Breach of Warning Low Limit status.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.35.0

Non-volatile

ssTrapOnBooleanCriticalEnable

DESCRIPTION: A zero value disables this trap. A value of one enables this trap. When enabled, this trap is sent when the agent detects that the currently indexed variable on the currently indexed device enters a Breach of Boolean Critical Limit status. It will be sent periodically using the time interval in minutes specified by ssTrapOnBooleanCriticalInterval.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.36.0

Non-volatile

ssTrapOnBooleanCriticalInterval

DESCRIPTION: The time interval in minutes between traps when the agent detects that the currently indexed variable on the currently indexed device enters a Breach of Boolean Critical Limit status.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.37.0

Non-volatile

ssTrapOnReturnToNormalEnable

DESCRIPTION: A zero value disables this trap. Any other value enables the trap. When enabled, this trap is sent only once.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.38.0

Non-volatile

ssEmailOnScalarCriticalSubject

DESCRIPTION: This is the subject line of the email that will be sent when the currently indexed variable on the currently indexed device enters Breach of Critical High Limit status or Breach of

Critical Low Limit status. The subject line can also contain the dollar variables: $L, $U, $R, and $T. The dollar variable $L, will be expanded to the currently indexed device's location. The dollar variable $U, will be expanded to the location of the Alert appliance. The dollar variable $R, will be expanded into the reading of the currently indexed variable on the currently indexed device. The dollar variable $T, will be expanded into the current date and time.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.39.0

Non-volatile

ssEmailOnScalarCriticalMessage

DESCRIPTION: This is the email message that will be sent when the currently indexed variable on the currently indexed device enters Breach of Critical High Limit status or Breach of Critical Low Limit status. The message line can also contain the dollar variables: $L, $U, $R, $T and $N. The dollar variable $L, will be expanded to the currently indexed device's location. The dollar variable $U, will be expanded to the location of the Alert appliance. The dollar variable $R, will be expanded into the reading of the currently indexed variable on the Alert appliance. The dollar variable $T, will be expanded into the current date and time. Finally, the dollar variable $N, will be expanded into a newline character so that the message is easier to read

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.40.0

Non-volatile

ssEmailOnScalarCriticalAddresses

DESCRIPTION: This is a comma separated list of email recipients that will be sent an email when the currently indexed variable on the currently indexed device enters Breach of Critical High Limit status or Breach of Critical Low Limit status. For example: user@yourcompany.com, user2@yourcompany.com.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.41.0

Non-volatile

ssEmailOnScalarCriticalEnable

DESCRIPTION: A zero value disables this email alert. A value of one enables this email alert. When enabled, this email is sent when the currently indexed variable on the currently indexed device enters Breach of Critical High Limit status or Breach of Critical Low Limit status. It will be sent periodically using the time interval in minutes specified by ssEmailOnScalarCriticalInterval.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.42.0

Non-volatile

ssEmailOnScalarCriticalInterval

DESCRIPTION: The time interval in minutes between emails when the currently indexed variable on the currently indexed device enters Breach of Critical High Limit status or Breach of Critical Low Limit status.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.43.0

Non-volatile

ssEmailOnScalarWarningSubject

DESCRIPTION: This is the subject line of the email that will be sent when the currently indexed variable on the currently indexed device enters Breach of Warning High Limit status or Breach of Warning Low Limit status. The subject can also contain the dollar variables: $L, $U, $R, and $T. The dollar variable $L, will be expanded to the currently indexed device's location. The dollar variable $U, will be expanded to the location of the Alert appliance. The dollar variable $R, will be expanded into the reading of the currently indexed variable on the currently indexed device. The dollar variable $T, will be expanded into the current date and time.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.44.0

Non-volatile

ssEmailOnScalarWarningMessage

DESCRIPTION: This is the message of the Email that will be sent when the currently indexed variable on the currently indexed device enters Breach of Warning High Limit status or Breach of Warning Low Limit status. The message line can contain the dollar variables: $L, $U, $R, $T and $N. The dollar variable $L, will be expanded to the currently indexed device's location. The dollar variable $U, will be expanded to the location of the Alert appliance. The dollar variable $R, will be expanded into the currently indexed variable on the currently indexed device's current reading. The dollar variable $T, will be expanded into the current date and time. Finally, the dollar variable $N, will be expanded into a newline character so that the message is easier to read

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.45.0

Non-volatile

ssEmailOnScalarWarningAddresses

DESCRIPTION: This is the comma separated list of email recipients that will be sent an email when the currently indexed variable on the currently indexed device enters Breach of Warning High Limit status or Breach of Warning Low Limit status. For example: user@yourcompany.com, user2@yourcompany.com.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.46.0

Non-volatile

ssEmailOnScalarWarningEnable

DESCRIPTION: A zero value disables this email alert. A value of one enables this email alert. When enabled, this email is sent when the currently indexed variable on the currently indexed device enters Breach of Warning High Limit status or Breach of Warning Low Limit status. It will be sent periodically using the time interval in minutes specified by ssEmailOnScalarWarningInterval.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.47.0

Non-volatile

ssEmailOnScalarWarningInterval

DESCRIPTION: The time interval in minutes between emails when the currently indexed variable on the currently indexed device enters Breach of Warning High Limit status or Breach of Warning Low Limit status.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.48.0

Non-volatile

ssEmailOnBooleanCriticalSubject

DESCRIPTION: This is the subject line of the email that will be sent when the currently indexed variable on the currently indexed device enters Breach of Boolean Critical Limit status. The subject can also contain the dollar variables: $L, $U, $R, and $T. The dollar variable $L, will be expanded to the currently indexed device's location. The dollar variable $U, will be expanded to the location of the Alert appliance. The dollar variable $R, will be expanded into the currently indexed variable on the currently indexed device's current reading. The dollar variable $T, will be expanded into the current date and time.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.49.0

Non-volatile

ssEmailOnBooleanCriticalMessage

DESCRIPTION: This is the message of the email that will be sent when the currently indexed variable on the currently indexed device enters Breach of Boolean Critical Limit status. The message line can also contain the dollar variables: $L, $U, $R, $T and $N. The dollar variable $L,

will be expanded to the currently indexed device's location. The dollar variable $U, will be expanded to the location of the Alert appliance. The dollar variable $R, will be expanded into the currently indexed variable on the currently indexed device's current reading. The dollar variable $T, will be expanded into the current date and time. Finally, the dollar variable $N, will be expanded into a newline character so that the message is easier to read

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.50.0

Non-volatile

ssEmailOnBooleanCriticalAddresses

DESCRIPTION: This is a comma separated list of email recipients that will be sent an email when the currently indexed variable on the currently indexed device enters Breach of Boolean Critical Limit status. For example: user1@ABC.com, user2@ABC.com.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.51.0

Non-volatile

ssEmailOnBooleanCriticalEnable

DESCRIPTION: A zero value disables this email alert. A value of one enables this email alert. When enabled, this email is sent when the currently indexed variable on the currently indexed device enters Breach of Boolean Critical Limit status. It will be sent periodically using the time interval in minutes specified by ssEmailOnBooleanCriticalInterval.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.52.0

Non-volatile

ssEmailOnBooleanCriticalInterval

DESCRIPTION: The time interval in minutes between emails when the currently indexed variable on the currently indexed device enters Breach of Boolean Critical Limit status.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.53.0

Non-volatile

ssEmailOnReturnToNormalSubject

DESCRIPTION: This is the subject line of the email that will be sent when the currently indexed variable on the currently indexed device enters Returned To Normal status. The subject can also contain the dollar variables: $L, $U, $R, and $T. The dollar variable $L, will be expanded to the

currently indexed device's location. The dollar variable $U, will be expanded to the location of the Alert appliance. The dollar variable $R, will be expanded into the currently indexed variable on the currently indexed device's current reading. The dollar variable $T, will be expanded into the current date and time.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.54.0

Non-volatile

ssEmailOnReturnToNormalMessage

DESCRIPTION: This is the message of the email that will be sent when the currently indexed variable on the currently indexed device enters Returned To Normal status. The message line can also contain the dollar variables: $L, $U, $R, $T and $N. The dollar variable $L, will be expanded to the currently indexed device's location. The dollar variable $U, will be expanded to the location of the Alert appliance. The dollar variable $R, will be expanded into the currently indexed variable on the currently indexed device's current reading. The dollar variable $T, will be expanded into the current date and time. Finally, the dollar variable $N, will be expanded into a newline character so that the message is easier to read

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.55.0

Non-volatile

ssEmailOnReturnToNormalAddresses

DESCRIPTION: This is a comma separated list of email recipients that will be sent an email when the currently indexed variable on the currently indexed device enters Returned To Normal status.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.56.0

Non-volatile

ssEmailOnReturnToNormalEnable

DESCRIPTION: A zero value disables this email alert. Any other value enables this email alert. When enabled, this alert is sent only once.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.57.0

Non-volatile

ssCommandOnScalarCriticalHigh

DESCRIPTION: This is the command-line string that will be executed by the shell when the currently indexed variable on the currently indexed device enters Breach of Critical High Limit status.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.58.0

Non-volatile

ssCommandOnScalarCriticalHighEnable

DESCRIPTION: A zero value disables this command line alert. A value of one enables this command line alert. When enabled, this command line is executed when the currently indexed variable on the currently indexed device enters Breach of Critical High Limit status. It will be sent periodically using the time interval in minutes specified by ssCommandOnScalarCriticalHighInterval.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.59.0

Non-volatile

ssCommandOnScalarCriticalHighInterval

DESCRIPTION: The time interval in minutes between command line execution when the currently indexed variable on the currently indexed device enters Breach of Critical High Limit status.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.60.0

Non-volatile

ssCommandOnScalarWarningHigh

DESCRIPTION: This is the command-line string that will be executed by the shell when the currently indexed variable on the currently indexed device enters Breach of Warning High Limit status.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.61.0

Non-volatile

ssCommandOnScalarWarningHighEnable

DESCRIPTION: This is the command-line string that will be executed by the shell when the currently indexed variable on the currently device enters Breach of Warning High Limit status.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.62.0

Non-volatile

ssCommandOnScalarWarningHighInterval

DESCRIPTION: The time interval in minutes between command line execution when the currently indexed variable enters Breach of Warning High Limit status.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.63.0

Non-volatile

ssCommandOnScalarWarningLow

DESCRIPTION: This is the command-line string that will be executed by the shell when the currently indexed variable on the currently indexed device enters Breach of Warning Low Limit status.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.64.0

Non-volatile

ssCommandOnScalarWarningLowEnable

DESCRIPTION: A zero value disables this command line alert. A value of one enables this command line alert. When enabled, this command line is executed when the currently indexed variable on the currently indexed device enters Breach of Warning Low Limit status. It will be sent periodically using the time interval in minutes specified by ssCommandOnScalarWarningLowInterval.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.65.0

Non-volatile

ssCommandOnScalarWarningLowInterval

DESCRIPTION: The time interval in minutes between command line execution when the currently indexed variable enters Breach of Warning Low Limit status.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.66.0

Non-volatile

ssCommandOnScalarCriticalLow

DESCRIPTION: This is the command-line string that will be executed by the shell when the currently indexed variable on the currently indexed device enters Breach of Critical Low Limit status.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.67.0

Non-volatile

ssCommandOnScalarCriticalLowEnable

DESCRIPTION: A zero value disables this command line alert. A value of one enables this command line alert. When enabled, this command line is executed when the currently indexed variable on the currently indexed device enters Breach of Critical Low Limit status. It will be sent periodically using the time interval in minutes specified by ssCommandOnScalarCriticalLowInterval.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.68.0

Non-volatile

ssCommandOnScalarCriticalLowInterval

DESCRIPTION: The time interval in minutes between command line execution when the currently indexed variable enters Breach of Critical Low Limit status.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.69.0

Non-volatile

ssCommandOnBooleanCritical

DESCRIPTION: This is the command-line string that will be executed by the shell when the currently indexed variable on the currently index device enters Breach of Boolean Critical Limit status.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.70.0

Non-volatile

ssCommandOnBooleanCriticalEnable

DESCRIPTION: A zero value disables this command line alert. A value of one enables this command line alert. When enabled, this command line is executed when the currently indexed variable on the currently indexed device enters Breach of Boolean Critical Limit status. It will be sent periodically using the time interval in minutes specified by ssCommandOnBooleanCriticalInterval.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.71.0

Non-volatile

ssCommandOnBooleanCriticalInterval

DESCRIPTION: The time interval in minutes between command line execution when the currently indexed variable enters Breach of Boolean Critical Limit status. A zero value disables this command.

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.72.0

Non-volatile

ssCommandOnReturnToNormal

DESCRIPTION: This is the command-line string that will be executed by the shell when the currently indexed variable on the currently indexed device enters Returned To Normal status.

TYPE: String

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.73.0

Non-volatile

ssCommandOnReturnToNormalEnable

DESCRIPTION: A zero value disables this command alert. Any other value enables this command alert. When enabled, this alert is sent only once."

TYPE: Integer

ACCESS: Read/Write

OID .1.3.6.1.4.1.15848.1.74.0

Non-volatile

Security Considerations

IMPORTANT - If you are planning to expose your Alert appliance to the Internet, Sensorsoft recommends that you do so through a separate firewall device that is capable of protecting your network from various hacker attacks, including SYN flooding, Ping of Death, IP Spoofing, etc. These types of attacks may cause Sensorsoft Alert to respond unexpectedly, or cause it to fail.

Multi-Level User Access

Your Alert appliance offers two levels of user access to allow some users to view only current monitored item information, while allowing other users to fully administer Alert.

IMPORTANT - Sensorsoft recommends that you only login to the Alert web interface using the ruser account when accessing Alert over the Internet. This will protect your admin password from being sent as clear text, as is described in the section *Password Encryption*.

Password Encryption

Your Alert appliance stores both its admin and ruser passwords in encrypted form to ensure that the passwords cannot be easily read without the use of the decryption algorithm.

IMPORTANT - Passwords are not encrypted as they are traversing the network from your web browser to the Alert appliance. An individual or hacker that is sniffing the network will be able to read this information as clear text.

User Definable Web Server Port

The Internet Assigned Numbers Authority (IANA) has defined TCP port 80 as the international standard TCP port for web servers. If you are using the Sensorsoft Alert appliance on the Internet you may wish to change this port to add an increased layer of security. You have the option to set this port from 1 to 65535, but Sensorsoft recommends that you choose a port between 1024 and 65535, as ports 1 through 1023 are reserved for other "well known" protocols. To change the web server port number of your Alert appliance, follow the procedure below:

1. Connect to the Alert appliance through Secure Shell or through the serial console. If the Alert appliance has not been configured with valid IP settings, then you must connect to it through the serial console (See the section *Connecting to the Alert Serial Console*).
2. Login as: **root**
3. At the command prompt, type **stopalert** and then press **Enter**.
4. Using **vi**, set the desired port number in the file **/etc/websport.conf**.
5. After editing /etc/websport.conf, close vi to return to the command prompt.
6. At the command prompt, type **saveconf** and then press **Enter**.
7. At the command prompt, type **reboot** and then press **Enter**. The Alert appliance will now reboot and will be online in one minute. After the Alert appliance has rebooted, its web interface will be accessible through the newly defined port.

Trouble Shooting

General Problems

Cannot access the web interface anymore

If you cannot access the Alert appliance web interface, but still have IP access using ping and ssh, you likely have a corrupt script (settings) file. Login to the root account using ssh and run the ps command. You should be able to see many (7) alertd processes running. If not attempt to start alertd as follows:

```
/bin/alertd
```

If you get the error message "unsupported platform" you have a corrupt script file. If you have previously done a backup of the script file you can follow the procedure in the section entitled *Restore known good script backup file to Alert appliance from a remote host*. Otherwise without having done a backup use the following procedure instead:

Place a copy of makemac in the /home directory and run it. Contact Sensorsoft Technical Support for a copy of makemac. Then be sure to delete makemac, run saveconf and reboot as follows:

```
# chmod +x /home/makemac
# /home/makemac
# rm –f makemac
# saveconf
# reboot
```

After the Alert appliance is allowed time to reboot you should be able to access its web interface.

Changes made to Alert appliance's settings were lost after the appliance was restarted.

If you have modified your Alert appliance's settings, then the new settings must be saved to the flash before the appliance is reboot or shutdown, otherwise your changes will be lost. Alert will automatically update its flash with the latest settings once every 5 minutes. If you need to reboot or shutdown the appliance immediately after making some changes to the settings, then to ensure that your changes will not be lost, you must use the **Reboot/Shutdown** page of the Alert web interface (Refer to the section *Appliance Shutdown and Reboot*).

Unable to launch the Sensorsoft Graphing Tool

To run the Sensorsoft Graphing Tool, you need to install the Sun Java Virtual Machine Version 1.4.1 or higher on your PC. If you are using Internet Explorer, you can check whether Java Virtual Machine Version 1.4.1 is installed doing the following:

1. Open Internet Explorer
2. In the **Tools** menus, look for the **Sun Java Console** option
3. If this option is not there, then you do not have Java Virtual Machine Version 1.4.1 or higher

If the Java Virtual Machine is installed and you are still unable to launch the Sensorsoft Graphing Tool, try logging out of the Alert web interface, and then in a new browser window, login again and click on the **Graph Data Files** link.

Sensorsoft device readings have erroneous values

This can occur if your Sensorsoft device has EEPROM failure or if it experiences large amounts of electro-magnetic interference. To check if EEPROM failure is the cause, go to the **Device Configuration** page of the Sensorsoft device by clicking on the device's **Description** hyperlink in the Main List View. On the bottom of the **Device Configuration** page you will see the event error counter for EEPROM Failures. If the EEPROM Failure counter is greater than zero, then the Sensorsoft device is having EEPROM failures and needs to be repaired.

The Sensorsoft Alert start date and time shown on the Alert web interface is wrong

This can occur if the Sensorsoft Alert date and time settings were wrong when the appliance booted up. To prevent this from happening, use NTP server for time synchronization (Refer to section *Setting Date and Time*). The date and time settings of the SSA7004 and SSA7008 model appliances are backed up by internal batteries. The SSA7001 appliance has no internal battery to maintain the date and time during power disconnection.

To correct the start date and time, first you must specify either the correct date and time manually or use a NTP server (Refer to section *Setting Date and Time*). If you have a SSA7001model appliance, then you must use a NTP server. Then, reboot Alert through the Alert web interface (Refer to the section *Safe Reboot / Shutdown*).

View Monitor List Error Messages

The View Monitor List will display error messages if your Alert appliance is having problems in communicating with a monitored device or if it detects a device is malfunctioning. The following is a list of common error messages and their solutions:

OFF LINE – TCP Connection Problem

The TCP port that is sharing the device may not be open. Take the following steps to fix the problem:

1. The fastest way to solve this problem is to stop monitoring this port, and then restart monitoring it. To stop monitoring the port, go to the **Administration** page and in the **Port Settings** table, clear the **Enable Monitor** checkbox, and click **Save Changes**. To restart monitoring, go back to the **Administration** page and in the **Port Settings** table, check the **Enable Monitoring** checkbox, and click **Save Changes**. Go to the **View Monitoring List** page and refresh it a few times to see if the error message is gone.
2. If the error message is still there after 1 minute, then you should reboot your Alert appliance. Remember to use the Alert web interface to safely reboot your appliance or else your settings may not be saved to the flash (Refer to the section *Appliance Shutdown and Reboot*).
3. If the error message persists, then click the **About** hyperlink on the left side of the web page. Check the software version number. If the version number is below 1.0.69, then you need to upgrade to the latest firmware (Refer to section *Upgrading the Firmware on your Alert Appliance*).

TIMEOUT – Device Not Responding

There are two possible causes of this error:

1. Other clients such as SCOM and Remote Watchman Enterprise may be monitoring this device through the Alert appliance's device sharing TCP ports. This in turn can cause the Alert appliance to have occasional connection problems to the device because only one client is allowed to connect to a particular device at anytime. If this is the cause, the error message will come and go periodically.

2. The monitored device is not properly connected or is damaged. First, make sure the device is properly connected to the port (Refer to the section *Connecting Sensorsoft Devices to the Alert Appliance*). If you are certain the device is properly connected, and yet the error message still appears, then the device or the serial cable may be physically damaged.

EEPROM FAILURE

The EEPROM on the device is malfunctioning due to physical damage and needs to be repaired. You may also notice abnormal readings from the device.

LOW SUPPLY VOLTAGE

The device does not have enough voltage to ensure proper, uninterrupted operation. To solve this problem, power the sensor using a 9 volt DC adapter. If the problem still persists, it indicates that the device has incurred physical damage and needs to be repaired.

TAMPER DETECTED

The device cannot read its probe or sensing element. This may indicate the device is experiencing a lot of electro-magnetic interference which could prevent it from reading its probe or sensing element properly. It is also possible that the probe or sensing element is damaged.

Email Problems

If your Alert appliance is having problems in send emails, you should in all cases find out the error message that is logged in your **smtp.log** file. Refer to section *Viewing Log Files* for how to view **smtp.log**. The following is a list of common errors and their solutions.

The SMTP address is incorrect

You have specified an invalid SMTP server address or the SMTP server is not online. Refer to section *SMTP Settings* for how to set the SMTP server address.

The recipient's email address or the sender's email address is incorrect

The recipient email address you have specified may be invalid. If you have specified multiple recipients, make sure that their email addresses are delimited by commas. You may also have specified an invalid sender email address. Most SMTP servers require the sender email address to be valid. See the section *SMTP Settings* for how to set the sender email address.

The sender's email address is incorrect

You have specified an invalid sender email address. Most SMTP servers require the sender email address to be valid. See the section *SMTP Settings* for how to set the sender email address.

The recipient's email address is incorrect

The recipient email address you have specified is invalid. If you have specified multiple recipients, make sure that their email addresses are delimited by commas.

Paging Problems

Please note that the paging feature is not available on the SSA7001 model appliance. If you are using SMS paging, it is important to note that most SMS providers impose a maximum limit on the number of characters that a message may contain, and will truncate the message to fit the maximum length. You should therefore find out from your SMS provider what the maximum message length is.

If you are experiencing problems sending a page, you should in all cases find out what error message is being sent to your **pager.log** file. See the section *Viewing Log Files* for how to view **pager.log**. The following is a list of common errors and their solutions.

No valid modem port has been setup

You have not specified which Alert serial port the modem is connected to. Refer to the section *Setting up Pager Alerts* for how to specify the modem port.

Timeout, modem did not respond

You should verify that the modem is properly connected and that you have the proper modem type selected on the **Administration** page. If your modem has DIP switches, ensure that they reflect the settings shown in *Appendix D*.

Modem setup string error

You should verify that the modem is properly connected and that you have the proper modem type selected on the **Administration** page. If your modem has DIP switches, ensure that they reflect the settings shown in *Appendix D*.

Unexpected response from modem

You should verify that the modem is properly connected and that you have the proper modem type selected on the **Administration** page. If your modem has DIP switches, ensure that they reflect the settings shown in *Appendix D*.

Modem timed out with NO CARRIER

The modem dialed but did not connect to another modem at the destination phone number. You should verify the modem pool phone number with your paging service provider.

Modem reported error in dial string

The dial command caused the modem to return an error. You should verify that you have the proper modem type selected on the **Administration** page. If your modem has DIP switches, ensure that they reflect the settings shown in *Appendix A*.

Modem reported NO DIAL TONE

You should verify that the phone line is securely plugged into the proper jack on the modem and the wall. You should also verify that the dial tone is steady. An intermittent dial tone can be caused by a message indication from your call answer service. You may wish to disable the call answer service feature.

Timeout, modem did not connect

The modem dialed but did not connect to another modem at the destination phone number. You should verify the modem phone number with your paging service provider.

If you still receive this error message after trying the above, you should contact your paging service provider to report a problem.

Getting Help

Limited Warranty

Sensorsoft Corporation warranties this Sensorsoft product to be free from manufacturing defects for a period of one year. This includes parts and labor. All shipping and brokerage fees are your responsibility when returning a Sensorsoft product for warranty claims. The following will void the warranty and 30 day money back guarantee:

- signs of water or chemical damage
- cracks to the housing
- signs of tampering or reverse engineering

Technical Support

If in the unlikely event you should have problems setting up or using Sensorsoft Alert, and the previous sections have failed to provide a solution, we offer technical support to help you overcome your difficulties.

You will receive three (3) support incidents (telephone calls or emails) with your initial purchase of Sensorsoft Alert. After these incidents are used, you must purchase a support package or pay a charge-per-incident fee. None of the included support incidents can be used for those wishing to obtain support to write their own software; this is available on a charge-per-incident basis only.

Before contacting Sensorsoft Technical Support:

Go through the *Troubleshooting Guide* in the previous sections of this manual. Even if a direct answer to your question is not found there, it will be helpful for the support technician if you are able to provide information obtained from the diagnostic and troubleshooting process. Please ensure the problem is directly related to the Sensorsoft Alert software.

World Wide Web: http://www.sensorsoft.com
E-mail: support@sensorsoft.com

30 Day Money Back Guarantee

If for any reason you want to return a Sensorsoft product for a refund, you can do so within 30 days (calendar days) of your purchase. The refund does not include shipping or brokerage fees you may have incurred or paid.

Returns

If returning a product or item, please keep in mind the follow guidelines:

- Contact Sensorsoft for an RMA number (Return Material Authorization).
- Provide a detailed explanation or reason for returning the product.
- Return shipments that bear no RMA number (on the outside of the package) or are not prepaid for shipping/clearing charges, will be refused.

Appendix A - Using Dollar Variables in Messages

You will notice that the Email Subject Line, Email message line and Pager Message Line contain dollar variables (e.g $R, $U, $T, $L and $N). When the messages are sent, these dollar variables will be substituted with dynamic data. Below is list of dollar variables that can be used.

$R – Reading of the variable that caused the alert

$U – Location of the Sensorsoft Alert appliance

$T – Date and time at which the alert was sent

$L – Location of the SSD that caused the alert

$N – Inserts a new line in the text (do not use in email subject and pager message)

Appendix B - Controlling the SR6171J Sensorsoft Relay using Command Lines

The SR6171J Sensorsoft Relay can be turned on or off using a command line alert. An example command line to turn ON a SR6171J Sensorsoft Relay connected to serial port 4 of the Sensorsoft Alert appliance is:

```
scom –Q /bin/SR6171_ON.ini ttyS4
```

Similarly, an example of the command line used to turn OFF the SR6171J Sensorsoft Relay connected to serial port 4 of the Sensorsoft Alert appliance is:

```
scom –Q /bin/SR6171_OFF.ini ttyS4
```

In the command lines above, ttyS4 is the name used to access serial port 4. The relay can be connected to any serial port on the back of the Alert appliance. As an example, if the relay was connected on serial port 8, use ttyS8 in the command line.

IMPORTANT - In order for the above command lines to work, you need to disable monitoring on the port where the relay is connected. This is done by clearing the **Enable Monitoring** checkbox in the **Port Settings** table located at the top of the **Administration** page.

Appendix C - Pager Tutorial

Sensorsoft Alert supports three methods that can be used to issue alerts to your paging device. The following section will help you determine what method of delivery you can use.

What type of paging device do you have?

There are four main types of paging devices:

1. Digital cell phones with text messaging service
2. Alphanumeric pagers
3. Numeric pagers
4. Two-way Email Pagers (e.g. RIM Blackberry)

What delivery method does your paging service provider use to send messages to your paging device?

There are five main methods that are used to deliver messages to your paging device:

A. I have software for my computer that sends messages to my pager using my modem.

B. I use one paging device to send messages to a second paging device.

C. I dial the pager's phone number and wait for a voice that tells me to punch-in my call-back phone number with a Touch Tone™ (DTMF) key pad.

D. I send an email to the paging device using an email address that was given to me by my paging service provider.

E. I go onto my paging service provider's web site and send a message using a web page.

What method should I use to have messages sent to my paging device?

Using your answers from the last two questions, you can find out what method you should be using to send messages to your paging device.

	A	B	C	D	E
1 Digital Phone	SMS	SMS	N/S	SMTP	SMS
2 Alphanumeric Pager	SMS	SMS	N/S	SMTP	SMS
3 Numeric Pager	SMS	SMS	N/S	SMTP	SMS
4 Two-way Email Pager	SMS	SMS	N/S	SMTP	SMS

N/S – Not Supported

Please note that your paging service provider may not make all of the above methods available to you.

SMS Paging

Sensorsoft Alert can use the TAP protocol to send SMS messages to your paging device using your computer's modem. **In order to setup SMS paging in your Alert appliance, you will need to call your paging service provider and ask them for**:

- Their modem pool phone number.
- Your pager ID and any special formatting that is required.

The formatting of the pager ID varies from provider to provider. In most cases, you will find that your pager ID is the paging device's phone number. The format of the ID also varies. Some paging providers will not accept the ID if the area code is missing, while others will not accept the pager ID if hyphens are used to separate the numbers. You will need to enter the pager ID into Alert exactly like your paging service provider requires.

Most SMS providers impose a maximum limit on the number of characters that a message may contain, and will truncate the message to fit the maximum length.

SMTP Paging

If your paging service provider uses the SMTP protocol to send messages to your paging device, then you do not need to configure the paging portions of Sensorsoft Alert. In this case, we recommend using the email messaging feature of Sensorsoft Alert. Use the email address that was provided by your paging service provider.

Appendix D - Modem DIP Switch Settings

Modem DIP switch settings required for use with Sensorsoft Alert Paging

If you have a 3Com or U.S. Robotics modem with DIP switches, please make sure they reflect the required settings shown below. If you have another brand of modem that has DIP switches, please make sure they reflect the settings shown in the Function column:

DIP Switches (External Modems with DIP Switches Only)

Switch	Position	Function
1	OFF - UP	Normal DTR operations
2	OFF - UP	Result codes are words
3	ON - DOWN	Enable result codes
4	ON - DOWN	Echo disabled
5	ON - DOWN	Auto Answer disabled
6	OFF - UP	CD reflects state of carrier
7	OFF - UP	On power-up load user definition
8	ON - DOWN	Modem operates in smart mode

Appendix E – Alert Serial Port Pin-outs

The following table specifies the serial port pin-outs for SSA7001, SSA7004 and SSA7008. This information can be used to build your own cables to interface with Alert serial ports.

RS232 Signal	SSA7001 (DB9M)	SSA7004 / SSA7008 (RJ45)
TxD	3	3
RxD	2	6
DTR	4	2
DSR	6	8
DCD	1	7
RTS	7	1
CTS	8	5
Gnd	5	4

Appendix F – Using XML Output to Move Data to other Applications

Accessing the XML page

This section describes how to use the XML output capability of Sensorsoft Alert to move live data to other software applications.

To view the XML page, login to Alert's web interface as **ruser** or **admin**. From the Monitor List page, click the hyperlink **View in XML** at the top right corner. This will open a new web browser window containing the XML page.

An XML schema (XSD) page is also available. The XML schema defines the XML's hierarchy and data types. The schema file is used by automated readers to validate the XML output. Once you are logged into web interface you can access the XML schema (XSD) page, using the following URL:

http://<AlertApplianceIPAddress>/goform/main.xsd

To access the XML page from another software application, it will need to do the following:

1. Send the following HTTP Get request to Alert's web server port:

   GET /goform/CheckLogin?login=ruser&password=**<password>** HTTP/1.1

   Replace the above **<password>** string with the Alert appliance's ruser password.

2. Alert's web server will then respond with the following headers:

   HTTP/1.0 302 Redirect
   Server: GoAhead-Webs
   Date: Mon Mar 27 10:52:22 2006
   Pragma: no-cache
   Cache-Control: no-cache
   Content-Type: text/html
   Location: http://alertIP/read/main.asp
   Set-Cookie: sessionId=**<SessionIDValue>**; path=/

3. Your application is now logged in. In the headers above, <**SessionIDValue>** is the sessionID cookie passed back from the web server. Your application must record the <**SessionIDValue>** string in its memory. The next step will tell you what to do with this recorded value.

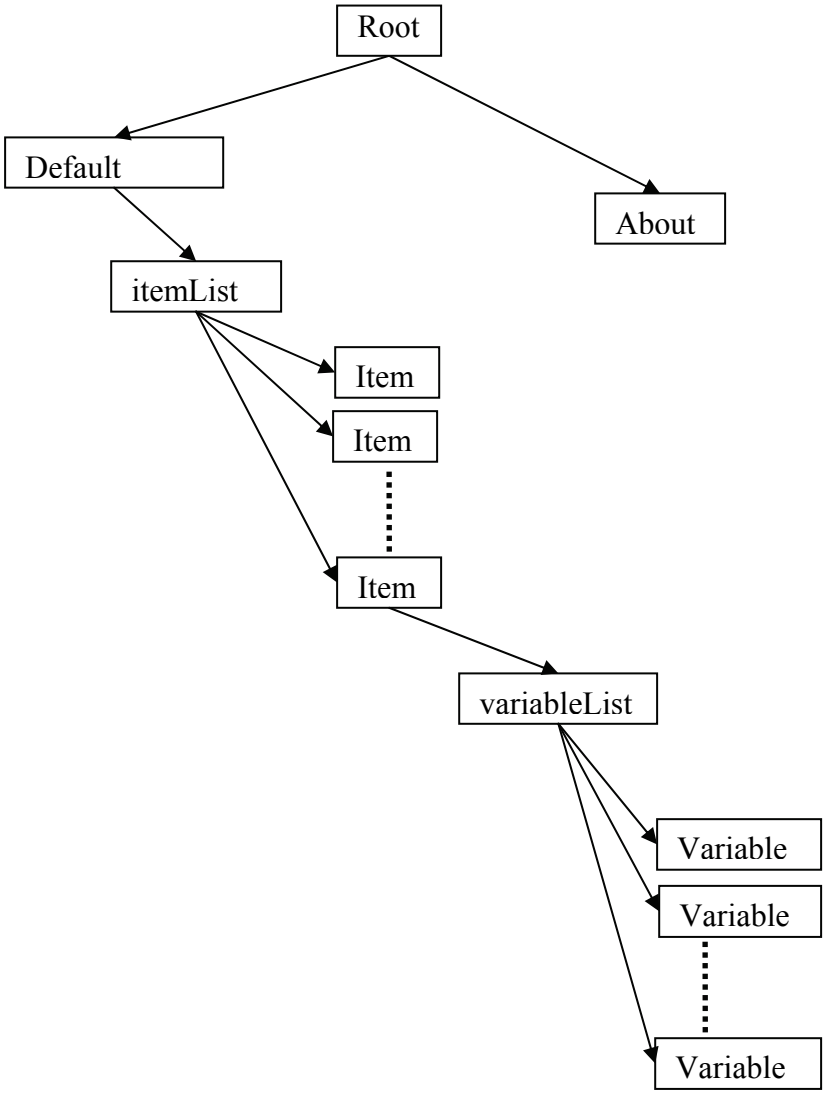
4. To request the XML page, send the following HTTP GET request:

   GET /goform/main.xml HTTP/1.1
   Cookie: sessionId=**<SessionIDValue>**

   Replace the above **<SessionIDValue>** string with the **<SessionIDValue>** that your application has recorded from Alert's last response. The web server in response will then send the XML page to your application.

XML data organization

This following tree diagram illustrates how data is organized in the XML page:



Data pertaining to each monitored item is located in a separate **Item** sub-tree under **\Root\Default Group\Items List**. Each **Item** sub-tree has a **variableList** sub-tree that contains the item's variable information. The data for each monitored variable is located in a separate **Variable** sub-tree under **variableList**. Please note that only variables that are shown on the **Monitor List** page will be listed under **variableList.** To select which item variables are to be shown on the Monitor List page, please refer to the section *Displaying Device Variables on the View Monitor List*.

Appendix G – Setting up a Routine Email Notification within the Linux shell

The following Linux shell script allows your Alert appliance to email a periodic sensor reading to reassure you that the appliance is working as expected. If the alertd or scomd processes are not running this shell script will also email a critical alert informing you that appropriate action is required. To install this shell script requires the user to have experience with Linux shell commands and the vi editor.

This shell script uses the sensor's first variable during the notification. If you are using a ST61XX thermometer on the sensor port you will receive a temperature sensor reading in Celsius. If you are using a SS6610 temperature/humidity meter on the sensor port you will receive a humidity sensor reading in %RH. If you are using a Boolean sensor such as SS6201/SP6400/SS6402 you will receive a state string reading (i.e. DRY, PWR_OK or OPEN).

1. Login to the Sensorsoft Alert appliance using an ssh tool like putty (port 22). The default login and password is "root" and "sensorsoft" respectively.

2. Using vi create a shell script file /home/routine_notify.sh and add the following content to it. Edit the sendmail command line to use the correct email addresses and mailserver address for your network. If you are using a SS6610 sensor on the sensor port, change the unit of measure C (for Celsius) to %RH (for humidity). If you are using a boolean sensor on the sensor port, remove the unit of measure, C from the shell script:

```
# start of routine notification shell script
agc=0
sgc=0
# count number of alertd processes
agc=`ps | grep alertd | grep –vc grep`
# count number of scomd processes
sgc=`ps | grep scomd | grep –vc grep`

# check that all the alertd threads are running, otherwise we have no
# environmental monitoring or alerting
if [ $agc -lt 6 ]
then
/usr/bin/sendmail -t you@yourdomain.com -f admin@yourdomain.com \
-s "Critical Alert - some or all alertd threads are not running" –m \
"Critical Alert - some or all alertd processes are not running. Login \
using ssh and troubleshoot immediately." -h mailserver

# check that the scomd process is running, otherwise we have no
# environmental monitoring or alerting
elif [ $sgc -lt 1 ]
then
/usr/bin/sendmail -t you@yourdomain.com -f admin@yourdomain.com \
-s "Critical Alert - scomd process is not running" -m "Critical \
Alert - scomd process is not running. Login using ssh and \
troubleshoot immediately." -h mailserver

# email the routine notification
else
/usr/bin/scomd -S ttyS1
Reading=`/usr/bin/scom -Q /home/scomsetup2.ini ttyS1`
/usr/bin/sendmail -t you@yourdomain.com -f admin@yourdomain.com \
-s "Routine Notification $Reading C" -m "This is a routine \
notification from Sensorsoft Alert, reading is $Reading C" \
```

```
-h mailserver
sleep 60  # prevents server bind address not available issue
/usr/bin/scomd -F /etc/scomd_port1.ini ttyS1

fi
# end of routine notification shell script
```

3. Run the following command to add execute privilege to the shell script:

```
# chmod +x  /home/routine_notify.sh
```

4. Using vi create a setup file /home/scomsetup2.ini and add the following content to it:

```
PortBitRate=1200
DelayAfterOpen=2
MaxRetriesOnError=2
ProbeTimeout=10
FormatDelimiter=new_line
Command=read_data
UnitofMeasure=C
```

5. Run the crontab scheduler edit command:

```
# crontab -e
```

   Add the following line to the crontab scheduler and save it (uses the vi editor). In this example the crontab scheduler runs the shell script at 7:00 AM everyday:

```
00 07 * * * /home/routine_notify.sh
```

6. Edit the file /etc/config_files and add the following line at the top of the file:

```
/var/cron/tabs/root
```

7. Save the above changes in flash memory using the following command:

```
# saveconf
```

8. Triple check all of the above files for correct entries. If additional changes are made, run the saveconf command again. To test the shell script for proper operation run it from the command line without using the crontab scheduler as follows:

```
# /home/routine_notify.sh
```